

ICS 35. xxx

CCS Lxx

团 体 标 准

T/ISC XXX—XXXX

法律从业人员人工智能使用与培训规范

Specification for artificial intelligence use and training of legal professionals

（征求意见稿）

XXXX – XX – XX 发布

XXXX – XX – XX 实施

目 次 中 国 互 联 网 协 会 发 布

前言	1
引言	2
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 人工智能	1
3.2 生成式人工智能	1
3.3 人工智能工具	1
3.4 法律从业人员	2
3.5 人工智能生成内容	2
3.6 敏感法律业务信息	2
3.7 人工复核	2
3.8 高风险使用场景	2
3.9 使用留痕	2
4 基本原则	2
4.1 合法合规原则	2
4.2 人类主导原则	2
4.3 审慎尽责原则	3
4.4 保密与最小必要原则	3
4.5 客户权益保护原则	3
4.6 公平与无歧视原则	3
4.7 责任不转移原则	3
4.8 过程可追溯原则	3
5 人工智能工具的选用与使用准备	3
5.1 一般要求	3
5.2 工具来源和适用范围	3
5.3 数据处理规则了解	4
5.4 组织准入和账户使用	4
5.5 使用前准备	4
5.6 工具变化和停止使用	4
6 输入信息处理要求	4
6.1 输入前识别	4
6.2 最小必要与脱敏	5
6.3 禁止和限制输入	5
6.4 输入信息的后续处理	5
7 法律业务场景中的使用要求	5
7.1 一般要求	5
7.2 法律法规及其他规范性文件检索	6
7.3 案例检索与类案分析	6
7.4 合同起草与审查	6
7.5 法律文书和法律意见起草	6
7.6 尽职调查与合规审查	6
7.7 案件分析和策略制定	7
7.8 法律咨询与客户沟通	7
7.9 法律研究和内部知识管理	7

7.10 高风险场景	7
8 输出复核与成果交付	7
8.1 一般要求	7
8.2 事实、证据和数据复核	8
8.3 法律依据和案例复核	8
8.4 逻辑、完整性和适用性复核	8
8.5 偏差、保密和知识产权复核	8
8.6 修改、确认和交付	8
8.7 告知和成果说明	9
9 职业伦理与禁止行为	9
9.1 独立判断和勤勉尽责	9
9.2 保密义务和利益冲突	9
9.3 诚实信用和真实陈述	9
9.4 禁止行为	9
10 使用记录、责任与异常处置	10
10.1 使用记录	10
10.2 记录保护和保存	10
10.3 法律从业人员责任	11
10.4 组织责任	11
10.5 错误输出处置	11
10.6 信息安全异常处置	11
10.7 客户权益补救	11
11 使用规范培训	12
11.1 培训目的和对象	12
11.2 培训内容	12
11.3 培训层级	12
11.4 基础级培训	12
11.5 应用级培训	13
11.6 管理级培训	13
11.7 专家级培训	14
11.8 培训实施	15
11.9 考核管理	15
11.10 培训记录和更新	15
12 监督与持续改进	15
12.1 一般要求	15
12.2 使用情况检查	15
12.3 问题纠正	16
12.4 培训效果评价	16
12.5 持续更新	16
附录 A （资料性） 法律业务场景人工智能使用风险参考表	17
A.1 使用说明	17
A.2 场景参考表	17
A.3 风险程度参考	18
附录 B （资料性） 人工智能工具使用前审查清单	18
B.1 使用说明	18

B.2 审查事项	19
B.3 审查结果处理	20
附录 C （资料性） 输入信息与输出内容复核清单	20
C.1 使用说明	20
C.2 输入信息审查清单	20
C.3 输出内容复核清单	21
C.4 复核结果处理	22
附录 D （资料性） 禁止及限制使用行为示例	22
D.1 使用说明	22
附录 E （规范性） 分层培训课程与考核要求	26

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

引 言

随着生成式人工智能、大语言模型等技术的发展，人工智能工具逐步应用于法律检索、案例分析、合同起草与审查、法律文书起草、尽职调查、合规管理、法律咨询和知识管理等法律业务场景，为法律从业人员处理信息和开展辅助性工作提供了新的工具。

人工智能在提升工作效率的同时，也可能产生虚假或者不准确的输出，并可能引发客户信息泄露、不当处理个人信息、引用虚构法律依据或者案例、算法偏差、不当依赖、知识产权争议以及责任边界不清等风险。法律业务具有较强的专业性，相关成果可能影响当事人的权利义务和法律服务质量。人工智能的使用不能替代法律从业人员依法或者依照职业规范应当作出的专业判断，也不改变法律从业人员应承担的保密、勤勉尽责和客户权益保护等义务。

为引导法律从业人员安全、合规、审慎地使用人工智能，有必要对工具选用、输入信息处理、法律业务场景使用、输出复核、成果交付、职业伦理、使用记录和风险处置等事项形成统一、可操作的要求。同时，有必要通过与岗位职责和使用场景相适应的培训，使法律从业人员理解相关规则，具备必要的风险识别、人工复核和规范操作能力。

本文件以法律从业人员使用人工智能的行为规范为主体，并规定相应的分层培训要求。相关培训以规范使用、风险识别、输出核验和必要操作为主要内容，不以人工智能模型开发或者综合技术能力培养为主要目的。

法律从业人员人工智能使用与培训规范

1 范围

本文件规定了法律从业人员使用人工智能的基本原则、工具选用与使用准备、输入信息处理、法律业务使用、输出复核与成果交付、职业伦理与禁止行为、使用记录与风险处置、培训以及监督改进等要求。

本文件适用于法律从业人员使用人工智能的活动及相关培训，也适用于律师事务所、企业法务部门、公证机构、仲裁机构、法律援助机构及其他相关组织开展人工智能使用管理和培训。

2 规范性引用文件

GB/T 41867—2022《信息技术 人工智能 术语》

3 术语和定义

下列术语和定义适用于本文件。

3.1 人工智能 **Artificial Intelligence;AI**

〈学科〉人工智能系统相关机制和应用的研究和开发。

3.2 生成式人工智能 **Generative Artificial Intelligence;GenAI**

是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。

3.3 人工智能工具

向用户提供人工智能功能，用于完成信息处理、内容生成、分析、检索或其他任务的软件、平台、服务或系统。

3.4 法律从业人员

从事律师、企业法务、合规、司法辅助、仲裁、公证及其他法律服务相关工作的人员。

3.5 人工智能生成内容

人工智能工具根据用户输入、系统指令、检索结果或其他信息生成、整理、改写、分析或推荐的内容。

3.6 敏感法律业务信息

在法律服务、法律管理或法律研究活动中形成、取得或处理的，未经授权不宜向无关人员或者不受控制的系统披露的信息。

注：敏感法律业务信息可以包括客户保密信息、案件信息、商业秘密、个人信息、未公开的交易信息和内部管理信息等。

3.7 人工复核

由法律从业人员对人工智能生成内容的事实、法律依据、逻辑、完整性、适用性及其他与使用目的有关的事项进行审查、核验、修改和确认的过程。

3.8 高风险使用场景

人工智能输出可能对当事人的重大权利义务、法律服务结论、诉讼或仲裁策略、重大交易或监管事项产生直接或者重大影响的使用场景。

3.9 使用留痕

对人工智能工具的使用人员、时间、目的、输入信息类别、输出用途、复核和交付等情况进行记录，以支持使用过程的核查和责任追溯。

4 基本原则

法律从业人员使用人工智能应遵循下列原则：

a) 合法合规。应遵守适用的法律法规、职业规范、监管要求、委托约定和所在组织的管理制度，不得以使用人工智能为由规避相关要求。

b) 人类主导。人工智能应作为辅助工具使用；依法或者依职业规范应由法律从业人员作出的专业判断、业务决策和最终确认，不应完全交由人工智能作出。

c) 审慎尽责。应了解所使用工具的基本功能、适用范围和已知局限，根据业务重要程度和可能后果确定使用方式和复核程度，未经必要复核不应直接采用人工智能生成内容。

d) 保密和最小必要。应履行保密义务，保护客户、案件及其他敏感法律业务信息；输入信息应限于完成特定任务所必需的范围，并采取适当保护措施。

e) 客户权益保护。人工智能的使用不应降低法律服务的专业标准，不应损害客户的知情权、选择权、保密权和其他合法权益；产生实质影响时，应依法依规履行告知或者授权要求。

f) 公平和无歧视。应关注生成内容中可能存在的偏见、歧视、刻板印象或者不合理差别待遇，不应直接采用存在前述问题且未经纠正的内容。

g) 责任不转移。应对采纳、修改、使用和对外提交的人工智能生成内容承担与其行为相应的责任，不得以系统错误、模型局限或者服务中断为由免除或者转移依法应承担的责任。

h) 过程可追溯。对重要或者高风险法律业务中的人工智能使用，应保留与风险相适应的记录，使关键使用、复核、审批和交付环节能够被核查。

5 人工智能工具的选用与使用准备

5.1 一般要求

法律从业人员使用人工智能工具前，应结合拟处理的业务类型、使用目的、输入信息的敏感程度和输出内容的用途，判断该工具是否适合使用。相关组织宜建立与其业务规模和风险相适应的人工智能工具使用管理要求。

5.2 工具来源和适用范围

法律从业人员宜选择来源明确、服务提供者可识别且适用范围相对清晰的人工智能工具。不宜使用来源不明、功能和数据处理规则不清晰，或者明显不符合保密要求的人工智能工具处理法律业务。

使用人工智能工具前，宜了解其主要功能、已知局限、输出内容的可靠性提示及服务提供者提供的使用规则。法律从业人员不应将工具的宣传、演示结果或者自动生成的说明直接视为法律业务结论的依据。

5.3 数据处理规则了解

处理客户材料、案件材料或者其他敏感法律业务信息前，法律从业人员应了解所使用工具对输入信息、对话记录和生成内容的处理规则，重点关注信息是否被保存、共享或者用于模型训练，以及是否提供访问控制、历史记录管理和删除等功能。

发现工具的数据处理规则与法律法规、职业规范、委托约定或者所在组织管理要求不相符的，不应使用该工具处理相关信息。

5.4 组织准入和账户使用

相关组织已建立人工智能工具准入或者账户管理要求的，法律从业人员处理客户材料、案件材料或者其他敏感法律业务信息时，应使用经组织允许的工具和账户。

未经所在组织允许，不应使用个人账户、共享账户或者未经批准的公共人工智能工具处理前款所述信息。

5.5 使用前准备

法律从业人员在使用人工智能工具前，应明确任务目的、预期用途和人工复核安排。对重要或者高风险业务，宜在使用前确定复核人员、复核方式以及是否需要履行审批或者告知程序。

法律从业人员应根据任务需要控制输入内容和使用范围，不应因便利而将人工智能工具用于与任务无关的材料处理或者作出超出工具适用范围的判断。

5.6 工具变化和停止使用

人工智能工具的功能、服务条款、数据处理规则或者安全措施发生重大变化时，法律从业人员和相关组织应重新判断其是否适合继续用于相关业务。

发现人工智能工具存在明显的安全隐患、严重错误输出或者其他可能损害客户权益和法律服务质量的情形时，应停止或者限制其在相应业务中的使用，并采取必要的核验、纠正或者报告措施。

6 输入信息处理要求

6.1 输入前识别

法律从业人员向人工智能工具输入信息前，应结合业务性质和使用目的，识别输入信息是否包含国家秘密、工作秘密、商业秘密、客户保密信息、个人信息、未公开案件信息、未公开交易信息、内部管理信息或者受知识产权保护的内容。

6.2 最小必要与脱敏

向人工智能工具输入信息应限于完成特定任务所必需的范围。不应为便利而输入与任务无关的完整案卷、完整客户材料或者其他完整文件。

在不影响任务完成的情况下，宜通过摘要、删除、替换、模糊化、脱敏或者结构化提取等方式减少原始信息输入。对能够使用公开信息、模拟信息或者经处理的信息完成的任务，宜避免输入原始敏感法律业务信息。

因任务需要输入完整案件材料、完整客户材料或者其他原始敏感法律业务信息的，应使用符合第5章要求且经所在组织允许的人工智能工具或处理环境，并采取与信息敏感程度相适应的访问控制、权限管理和其他保护措施。

6.3 禁止和限制输入

无论何种情况下，均不应向人工智能工具输入国家秘密、依法不得公开的信息、核心商业秘密以及其他依法禁止处理的信息。

使用客户材料、案件材料或者含有个人信息材料时，应符合保密义务、委托约定、客户授权、所在组织管理要求和相关规定。相关组织对特定信息或者特定工具另有禁止、限制要求的，法律从业人员应遵守。

6.4 输入信息的后续处理

法律从业人员应关注输入信息、对话记录和生成内容的保存、共享和删除情况。涉及输入信息保存、删除、共享、境外访问或者跨境处理的，应按照相关法律法规、职业规范、委托约定和所在组织制度执行。

因使用人工智能工具可能导致敏感法律业务信息被不当保存、共享、访问或者披露的，法律从业人员应及时停止相关使用，并按照所在组织制度采取报告、核验和补救措施。

7 法律业务场景中的使用要求

7.1 一般要求

法律从业人员应根据业务重要程度、输入信息的敏感程度、人工智能参与程度、输出内容的用途以及错误可能造成的后果，确定人工智能工具的使用范围、人工复核要求和必要的记录措施。

人工智能可用于法律业务中的信息整理、初步分析、文本生成和其他辅助性工作，但不应替代法律从业人员进行必要的事实调查、法律研究、专业分析和最终判断。

对重要或者高风险业务，法律从业人员应提高复核程度；相关组织可根据业务需要设置复核、审批或者其他控制措施。

7.2 法律法规及其他规范性文件检索

使用人工智能工具检索法律法规、司法解释、部门规章、地方性法规、规范性文件或者其他规则时，应核验文件名称、发布机关、条文内容、效力层级、现行有效状态和适用范围。

人工智能生成的法律依据仅可作为检索线索或者辅助材料使用。不应仅依据人工智能生成内容确认法律依据，也不应引用无法查证、已失效或者与所涉事项无关的法律依据。

7.3 案例检索与类案分析

使用人工智能工具进行案例检索、裁判观点归纳或者类案分析时，应核验案例是否真实存在，并核对案号、裁判机关、裁判日期、审级、裁判结果、裁判要旨及来源。

使用人工智能生成的案例分析结果时，应结合案件事实、证据情况、程序进展和适用规则进行判断，不应将其作为预测裁判结果或者作出诉讼、仲裁策略的唯一依据。

7.4 合同起草与审查

人工智能工具可用于辅助识别合同条款缺失、表述问题、权利义务不平衡、履行风险或者其他需关注事项。

法律从业人员使用人工智能生成或者审查合同内容时，应结合交易背景、当事人真实意思、商业安排、适用法律和风险承受能力进行实质审查和修改。不应将人工智能生成内容未经审查直接作为合同定稿。

7.5 法律文书和法律意见起草

使用人工智能工具起草诉讼文书、仲裁文书、法律意见书、律师函、法律备忘录或者其他法律文件时，应以已经核实的事实、证据和法律依据为基础。

法律从业人员应对人工智能生成内容进行实质性审查、修改和确认，确保文件内容与委托事项、案件事实、证据材料和适用规则相符。不应将人工智能生成的文书或者法律意见未经人工复核直接对外提交或者交付。

7.6 尽职调查与合规审查

人工智能工具可用于辅助材料分类、信息提取、问题识别、清单生成和报告初稿撰写。

使用人工智能工具开展尽职调查或者合规审查时，应核验相关信息的来源和准确性，并在成果中区分已经确认的事实、人工智能生成的归纳或者推断以及法律从业人员作出的专业判断。对关键事实、重大风险和结论性意见，应进行人工核验。

7.7 案件分析和策略制定

人工智能工具可用于辅助梳理争议焦点、分析已知事实和证据、列举可能的法律问题或者提示程序风险。

法律从业人员应结合案件材料、证据规则、程序进展、司法实践和客户目标独立判断。人工智能生成的分析、建议或者策略不应直接作为案件结论、诉讼或者仲裁策略的唯一依据。

7.8 法律咨询与客户沟通

使用人工智能工具辅助起草法律咨询意见、客户回复、沟通材料或者服务说明时，应由法律从业人员进行复核，确保内容准确、完整，并与客户的具体情况相适应。

不应使客户误认为人工智能工具可以独立提供正式法律意见或者替代法律从业人员。对人工智能的使用对法律服务过程、专业判断或者交付成果产生实质影响的，应按照本文件和有关约定履行相应的告知或者授权要求。

7.9 法律研究和内部知识管理

使用人工智能工具开展法律研究、整理内部知识或者制作培训材料时，应核验人工智能生成内容所涉及的法律规则、案例、数据和文献来源。

不应将未经核实的人工智能生成内容纳入对外发布的研究成果、内部知识库或者培训材料。使用受知识产权保护的内容时，应注意其使用权限和引用要求。

7.10 高风险场景

下列场景通常属于高风险使用场景：

形成重大法律意见、重大交易法律文件或者重大合规结论；

制定诉讼、仲裁、行政复议、行政诉讼或者其他争议解决策略；

涉及刑事案件、未成年人权益、自然人重大人身或者财产权益的事项；

用于监管申报、重大信息披露或者可能产生重大法律后果的对外文件；

其他错误使用可能对客户、当事人或者相关方造成重大不利影响的事项。

在高风险使用场景中使用人工智能工具时，应明确使用目的和范围，实施强化人工复核，并保留必要的使用和复核记录。相关组织可根据业务性质设置双重审核、分级审批或者其他控制措施。

8 输出复核与成果交付

8.1 一般要求

法律从业人员拟采纳、引用、提交、交付或者对外发布人工智能生成内容前，应根据内容用途、业务重要程度和风险程度进行人工复核。

人工复核应由具备相应法律专业知识并了解相关业务情况的法律从业人员实施。重要或者高风险法律业务中的人工智能生成内容，相关组织宜根据业务需要设置复核、审批或者双重审核安排。

8.2 事实、证据和数据复核

法律从业人员应核验人工智能生成内容涉及的主体、时间、地点、金额、事件、交易安排、证据材料和其他事实、数据是否准确，并与已掌握的材料相互印证。

对人工智能生成内容中无法从可靠来源核实的事实、证据或者数据，不应将其作为法律服务成果的依据或者对外陈述。

8.3 法律依据和案例复核

法律从业人员应核验人工智能生成内容所引用法律法规、司法解释、部门规章、规范性文件和其

他规则的名称、发布机关、条文内容、效力层级、现行有效状态和适用性。

引用案例时，应核验案例是否真实存在，并核对案号、裁判机关、裁判日期、审级、裁判结果、裁判要旨和来源。不应使用无法查证、虚构、失效或者不适用的法律依据、案例、数据或者文献。

8.4 逻辑、完整性和适用性复核

法律从业人员应审查人工智能生成内容的法律关系、论证逻辑、事实与结论之间的对应关系，以及结论是否与适用规则相符。

法律从业人员还应结合具体事项，审查人工智能生成内容是否遗漏重要事实、限制条件、例外情形、程序风险、反方观点或者其他可能影响结论的内容。

8.5 偏差、保密和知识产权复核

法律从业人员应审查人工智能生成内容是否含有偏见、歧视、刻板印象、误导性表述或者其他不当内容。

对拟对外使用的人工智能生成内容，还应审查其是否包含不应披露的客户信息、案件信息或者其他敏感法律业务信息，是否可能侵犯他人著作权、商标权或者其他合法权益，以及引用和署名是否符合有关要求。

8.6 修改、确认和交付

法律从业人员应根据复核结果对人工智能生成内容进行修改、补充、删除或者重新生成，并对最终使用的内容进行确认。

人工智能生成内容未经人工复核、必要修改和确认，不应作为正式法律服务成果对外提交或者交付。以人工智能生成内容为基础形成的法律服务成果，应由对该成果负责的法律从业人员依法或者依职业规范完成必要的签署、确认或者交付程序。

8.7 告知和成果说明

人工智能的使用对法律服务过程、专业判断或者交付成果产生实质影响，或者法律法规、职业规范、委托约定另有要求的，法律从业人员应履行相应的告知、授权或者说明程序。

法律从业人员不应将人工智能辅助形成的成果虚假表述为完全由人工完成，也不应夸大人工智能工具的功能、可靠性或者对法律服务成果作出误导性承诺。

9 职业伦理与禁止行为

9.1 独立判断和勤勉尽责

法律从业人员使用人工智能时，应保持专业独立，不应机械接受或者照搬人工智能生成内容。

法律从业人员不应因使用人工智能而减少必要的事实调查、证据审查、法律研究、专业分析或者沟通说明，也不应降低法律服务应有的专业标准。

9.2 保密义务和利益冲突

法律从业人员不应因人工智能工具使用便利而降低对客户信息、案件信息、商业秘密和内部资料的保密要求。

法律从业人员应关注人工智能工具的数据共享、模型训练、多用户环境或者服务提供者对信息的处理方式，是否可能导致客户信息不当利用、泄露或者利益冲突。发现存在前述风险且无法采取有效控制措施的，不应使用该工具处理相关业务。

9.3 诚实信用和真实陈述

法律从业人员不应使用人工智能生成、修改或者传播虚假的法律法规、案例、事实、证据、法律文件、签名、图像、音视频或者其他材料。

法律从业人员不应隐瞒已经发现且可能对客户权益、法律服务质量或者相关程序产生重大影响的人工智能使用错误或者风险。

9.4 禁止行为

法律从业人员不应实施下列行为：

- a) 向人工智能工具输入国家秘密、依法不得公开的信息、核心商业秘密以及其他依法禁止处理的信息；
- b) 在未取得合法授权，或者不符合业务必要、最小必要、安全可控、留痕管理等要求的情况下，将刑事案件、不公开审理案件、未成年人案件以及其他涉及工作秘密、商业秘密、个人信息、敏感个人信息或者客户保密信息的案件材料输入人工智能工具或者相关处理环境；
- c) 在不具备合法依据、业务必要性或者安全保密保障措施的情况下，将完整客户案卷、完整案件材料或者其他敏感法律业务信息输入人工智能工具或者相关处理环境；
- d) 未经核验引用人工智能生成的法律法规、案例、数据、文献或者其他信息；
- e) 将未经人工复核的人工智能生成内容直接作为正式法律服务成果交付、提交或者发布；
- f) 利用人工智能规避法律法规、职业规范、利益冲突审查、广告宣传要求或者其他监管要求；
- g) 将依法或者依职业规范应由本人作出的最终专业判断完全交由人工智能作出；
- h) 以人工智能生成、系统错误或者技术局限为由逃避、免除或者不当转移应承担的责任；
- i) 其他违反法律法规、职业规范、委托约定或者所在组织管理要求的不当使用人工智能的行为。

10 使用记录、责任与异常处置

10.1 使用记录

法律从业人员在重要或者高风险法律业务中使用人工智能工具时，应根据业务性质和风险程度保留必要的使用记录。相关组织可对其他业务场景的记录要求作出规定。

使用记录宜包括以下内容：

- a) 使用人员和使用时间；
- b) 所涉业务或者事项；
- c) 使用的人工智能工具及必要的版本、账户或者服务信息；

- d) 使用目的和输出用途；
- e) 输入信息的类别及采取的保护措施；
- f) 人工复核、审批或者授权情况；
- g) 最终使用、交付或者处置情况；
- h) 对最终成果负责的法律从业人员。

记录内容应与业务风险相适应。涉及敏感法律业务信息的，不应为留痕目的重复保存超出必要范围的原始材料、完整提示内容或者完整生成内容。

10.2 记录保护和保存

使用记录包含客户信息、案件信息、个人信息或者其他敏感法律业务信息的，应采取与其敏感程度相适应的访问控制、权限管理或者其他保护措施。

使用记录的保存期限应符合适用的法律法规、职业规范、委托约定、档案管理要求和所在组织制度。发生争议、投诉、调查或者风险事件时，应在适用范围内保全与该事项有关的必要记录。

10.3 法律从业人员责任

法律从业人员应对其使用人工智能工具的行为，以及其采纳、修改、使用、提交或者交付的人工智能生成内容承担相应责任。

法律从业人员发现人工智能生成内容存在重大错误、遗漏、虚构引用、保密风险或者其他可能影响法律服务质量和客户权益的情形时，应及时停止使用相关内容，并采取核验、修改、补充、删除、说明或者其他必要措施。

10.4 组织责任

相关组织宜根据业务特点建立人工智能工具使用、账户管理、输入信息处理、成果复核、使用记录、培训和风险处置等管理要求。

相关组织发现法律从业人员存在违反本文件、所在组织制度或者其他适用要求的人工智能使用行为时，应根据具体情况采取纠正、补训、限制使用权限或者其他必要措施。

10.5 错误输出处置

发现已经提交、交付、发布或者用于业务决策的人工智能生成内容存在重大错误、虚构引用、重要遗漏或者其他可能造成不利影响的情形时，相关法律从业人员应及时采取停止使用、核验、纠正和说明等措施。

需要对已经交付的法律服务成果作出补充、更正、撤回或者其他处置的，应根据具体业务、委托约定、职业规范和有关规定及时处理。相关组织可根据风险程度组织复核或者报告。

10.6 信息安全异常处置

发现因使用人工智能工具发生或者可能发生敏感法律业务信息泄露、越权访问、不当共享、异常传输或者其他安全异常时，法律从业人员应立即停止可能扩大影响的相关操作，并按照所在组织制度及时报告。

相关组织应根据事件性质和影响范围，采取核查、控制、补救、通知或者报告等措施。涉及个人信息、数据安全、保密义务或者其他法定报告事项的，应按照相关规定处理。

10.7 客户权益补救

人工智能工具的使用已经或者可能对客户、当事人或者其他相关方合法权益造成不利影响的，法律从业人员和相关组织应根据影响程度及时采取纠正、说明、补救或者其他必要措施。

相关处置不影响法律从业人员和相关组织依法或者依约应承担的责任。

10.8 风险事件报告与复盘

发生或者可能发生人工智能使用风险事件时，法律从业人员和相关组织宜按照下列步骤处置：

- a) 立即停止或者限制可能扩大影响的使用、传播、交付或者数据处理活动；
- b) 及时向所在组织或者相关责任主体报告，并保全与事件有关的必要记录和证据；
- c) 核查事件原因、影响范围、涉及人员、数据和业务成果，评估可能造成的法律和业务后果；
- d) 根据事件性质采取纠正、补救、通知、报告、权限调整、成果撤回或者其他必要措施；
- e) 事件处置完成后开展复盘，完善工具准入、使用流程、复核机制、培训内容和监督措施。

涉及法定报告、通知或者配合调查义务的，应按照适用的法律法规和有关规定执行。

11 使用规范培训

11.1 培训目的和对象

培训应使法律从业人员理解人工智能使用中的基本规则、风险边界和责任要求，能够安全、合规、审慎地使用人工智能开展法律辅助工作，并具备与其岗位职责和使用场景相适应的风险识别、人工复核和规范操作能力。

培训对象为本文件第 3.4 条规定的法律从业人员。培训实施方可根据法律从业人员的职业类型、岗位职责、业务场景和人工智能使用程度确定具体培训安排。

11.2 培训内容

11.2.1 法律从业人员培训内容

面向法律从业人员的培训应围绕其实际使用行为，包括下列内容：

- a) 规范使用要求，包括工具选用、保密义务、输入信息处理、客户权益、职业伦理、禁止行为、告知与授权、使用记录和责任承担；
- b) 风险识别与核验，包括识别虚假输出、虚构案例、失效法律依据、事实错误、逻辑缺陷、偏见歧视、保密和知识产权风险，并对输出进行人工复核；
- c) 必要操作，包括判断任务是否适合使用人工智能、选择适当工具、控制输入范围、提出清晰任务要求、保留必要记录和形成可复核成果。

培训可包含实现规范使用所必要的工具操作和基础任务指令练习，但不应以模型开发、模型训练、高阶提示词工程、智能体开发、通用办公效率或者综合人工智能技术能力培养为主要内容。

11.2.2 机构管理和培训实施人员培训内容

面向承担人工智能使用管理、风险控制、业务审核或者培训组织职责人员的培训，宜包括下列内容：

- a) 人工智能工具准入、账户权限、数据处理、使用范围和退出管理；
- b) 高风险业务识别、人工复核、审批、使用留痕和监督检查安排；
- c) 违规行为和风险事件的报告、调查、控制、补救与复盘；
- d) 分层培训、考核、培训记录和持续更新要求。

11.3 培训层级

使用规范培训分为基础级、应用级、管理级和专家级。培训层级应根据法律从业人员的岗位职责和人工智能使用场景确定，不宜仅依据职务、执业年限或者已完成的培训学时认定。

培训层级仅用于本文件项下的课程安排和培训考核，不构成法律执业资格、法律专业能力或者综合人工智能技术能力的等级认定。

基础级为其他层级的共同基础。参加较高级别培训的人员应掌握本层级及前序层级的相关内容。

11.4 基础级培训

11.4.1 培训对象

基础级培训适用于拟在法律服务、法律管理或者法律研究工作中接触或使用人工智能工具的法律从业人员。

11.4.2 课程要求

基础级课程宜包括：

- a) 人工智能的基本特征、常见功能和主要局限；
- b) 虚假输出、不当依赖等常见风险；
- c) 保密义务、信息输入底线和最小必要要求；
- d) 基本人工复核要求；
- e) 客户权益保护、禁止行为和个人责任。

11.4.3 考核方式

基础级考核宜采用知识测试和情境判断等方式，重点确认参训人员能够识别不宜输入的信息、明显不可信的输出和禁止使用行为。

11.5 应用级培训

11.5.1 培训对象

应用级培训适用于经常在法律检索、案例分析、合同审查、文书起草、尽职调查、合规管理、法律咨询或者其他法律业务场景中使用人工智能的法律从业人员。

11.5.2 课程要求

应用级课程宜包括：

- a) 工具和任务适用性判断；
- b) 输入信息识别、处理和必要保护；
- c) 主要法律业务场景的允许用途和使用边界；
- d) 事实、法律依据、案例、逻辑和完整性核验；
- e) 成果修改、确认、交付和客户告知；
- f) 使用留痕和典型风险事件处置。

课程应安排与法律业务有关的合规操作、输出复核或者案例练习。

11.5.3 考核方式

应用级考核应采用知识测试、案例判断和场景实操相结合的方式。场景实操应要求参训人员识别输入风险，判断是否适合使用人工智能，核验生成内容，并说明修改、采用或者不采用相关内容的理由。

11.6 管理级培训

11.6.1 培训对象

管理级培训适用于在律师事务所、企业法务部门、公证机构、仲裁机构或者其他相关组织中，承担人工智能使用管理、业务审核、风险控制、内部监督或者培训组织职责的法律从业人员。

11.6.2 课程要求

管理级课程宜包括：

- a) 人工智能工具准入和使用范围管理；
- b) 账户权限、输入信息和使用记录管理；
- c) 不同法律业务场景的风险控制；
- d) 人工复核、审批和监督检查安排；
- e) 违规行为处理和风险事件处置；
- f) 使用规范培训的组织实施。

11.6.3 考核方式

管理级考核宜采用案例分析、制度审查或者管理方案设计等方式，重点评价参训人员能否针对具体组织和业务场景识别管理缺陷、提出适当控制措施并处理风险事件。

11.7 专家级培训

11.7.1 培训对象

专家级培训适用于参与人工智能使用规范制定、重大法律业务风险审查、复杂事件调查、培训课程设计或者相关标准建设的法律从业人员。

11.7.2 课程要求

专家级课程宜包括：

- a) 复杂和高风险法律业务的人工智能使用边界；
- b) 人工智能使用中的疑难职业伦理问题；
- c) 系统性风险识别、评测和控制；
- d) 重大风险事件分析和复盘；
- e) 使用规范和培训方案设计；
- f) 标准实施及其效果评测。

11.7.3 考核方式

专家级考核宜采用复杂案例综合分析、规范或者培训方案设计和成果答辩等方式。参训人员拟承担培训工作的，可增加试讲或者模拟评审。

11.8 培训实施

培训可采用规则讲解、案例研讨、情境演练、合规操作和风险事件复盘等方式。应用级及以上培训应包含与相应岗位和场景有关的实践内容。

培训使用真实案例或者业务材料时，应进行适当处理并遵守保密、个人信息保护和所在组织管理要求。

培训人员应熟悉相关法律职业规范、本文件要求和人工智能使用中的主要风险。管理级和专家级培训可由法律实务人员与数据合规、信息安全等专业人员共同实施。

11.9 考核管理

培训实施方应根据培训层级制定考核方案，明确考核内容、方式、合格条件、评价要点和考核记录要求。学时完成情况不应作为培训合格的唯一依据。

考核不合格的，宜针对未达到的要求进行补充培训和再次考核。对考核中发现不具备相应规范使用能力的人员，相关组织可限制其使用特定工具或者处理较高风险业务。

本文件不规定各层级的统一最低学时和量化合格分数。相关要求可由培训实施方结合培训对象、课程内容和试点情况确定。

11.10 培训记录和更新

相关组织或者培训实施方应记录培训层级、培训时间、课程内容、培训人员、参训人员和考核结果。培训记录的保存和使用应符合相关管理要求。

人工智能工具、法律法规、职业规范、岗位职责或者使用风险发生重大变化，以及发生相关风险事件时，相关组织宜组织专项培训、补充培训或者重新评测。

12 监督与持续改进

12.1 一般要求

相关组织宜结合业务规模、人工智能使用范围和风险程度，对人工智能工具的使用和培训实施情况进行监督，并明确相应的管理职责。

监督和改进措施应与实际风险相适应，不宜对低风险、辅助性使用设置不必要的管理负担。

12.2 使用情况检查

相关组织宜定期或者根据需要检查以下事项：

- a) 是否使用经允许且适合相关业务的人工智能工具；
- b) 输入信息处理是否符合保密、最小必要和所在组织要求；
- c) 人工智能生成内容是否按照业务风险进行人工复核；
- d) 重要或者高风险业务是否履行必要的审批、告知和留痕要求；
- e) 是否存在违反职业伦理、禁止行为或者其他管理要求的情形；
- f) 培训对象、培训内容和考核安排是否与岗位和使用场景相适应。

检查可采用记录抽查、成果复核、人员访谈、案例复盘或者其他适当方式。检查过程中接触敏感法律业务信息的，应遵守相应的保密和信息保护要求。

12.3 问题纠正

发现人工智能使用或者培训实施不符合本文件要求的，相关组织应根据问题性质和影响程度采取纠正措施。

纠正措施可包括停止或者限制使用相关工具、补充人工复核、纠正或者撤回相关成果、完善记录、调整权限、修改内部规则、开展补充培训以及处置相关风险事件。

对重复发生或者可能造成重大不利影响的问题，相关组织宜分析原因，并对工具选择、业务流程、复核安排、培训内容或者监督方式进行相应调整。

12.4 培训效果评测

相关组织或者培训实施方宜结合培训考核结果、实际使用表现、违规情况和风险事件，对培训内容和实施效果进行评价。

发现受训人员虽完成培训但仍不能识别相应风险或者落实使用要求的，应调整课程、案例、实践安排或者考核方式，并根据需要组织补充培训。

12.5 持续更新

相关组织应关注人工智能工具、法律法规、职业规范和法律业务实践的变化，适时更新人工智能工具使用范围、内部管理要求、复核安排和培训内容。

发生重大错误输出、信息泄露、客户权益受损或者其他重要风险事件后，相关组织宜对事件进行复盘，并将相关经验用于完善使用规则、培训案例和风险防范措施。

附录 A
(资料性)
法律业务场景人工智能使用风险参考表

A.1 使用说明

本附录提供常见法律业务场景的人工智能用途、主要风险和控制措施示例，用于帮助法律从业人员理解和实施第 7 章、第 8 章的相关要求。

同一类法律业务可能因事项重要程度、输入信息敏感程度、人工智能参与程度、输出用途和错误后果不同而具有不同风险。使用表 A.1 时，宜结合具体业务进行判断，不宜仅根据场景名称确定风险程度。

A.2 场景参考表

表 A.1 法律业务场景人工智能使用风险参考表

法律业务场景	参考用途	主要风险	复核和控制重点	留痕建议
法律法规及规范性文件检索	生成检索线索、归纳条文、比较规则	虚构文件或条文、引用失效规则、遗漏适用条件	通过权威或可靠来源核验名称、发布机关、条文、效力状态和适用范围	重要事项可记录检索来源、核验结果和最终采用依据
案例检索与类案分析	查找案例线索、归纳裁判观点、比较案件要素	虚构案例、案号或裁判内容错误、忽略事实差异、过度预测裁判结果	核验案例真实性和来源，比较关键事实、争议焦点、审级和裁判理由	记录采用的案例来源以及关键核验事项
合同起草与审查	生成条款初稿、识别条款缺失或履约风险、辅助比较版本	忽略交易背景、权利义务失衡、遗漏特别约定、生成不适用条款	结合交易目的、商业安排、适用法律和客户风险偏好进行实质审查	重大交易可记录工具用途、重点修改和复核人员
法律文书和法律意见起草	生成结构或初稿、整理事实和论点、辅助文字修改	事实错误、虚构证据或依据、论证不完整、结论与委托事项不符	核对事实、证据、法律依据、请求或结论，完成实质修改和最终确认	对外提交或交付的重要成果宜记录复核、审批和最终责任人员
尽职调查与合规审查	材料分类、信息提取、问题识别、清单和报告初稿	材料遗漏、信息提取错误、将推断作为事实、未识别重大风险	核验信息来源，区分事实、系统归纳或推断和专业判断，复核重大风险	记录资料范围、人工智能用途、关键发现和人工核验情况
案件分析和策略制定	梳理争议焦点、列举法律问题、分析已有事实和证据、提示程序	不当预测结果、忽略证据限制或程序变化、策略与客户目标不符	结合完整案件材料、证据规则、程序进展和客户目标独立判断	高风险事项宜记录人工智能参与范围、复核和决策过程

	风险			
法律咨询与客户沟通	生成回复初稿、整理咨询问题、辅助形成服务说明	内容过于概括、忽略客户具体情况、形成误导或被误认为机器独立提供法律意见	核实客户事实和需求，由法律从业人员复核；必要时履行告知或授权	对客户权益有实质影响的，宜记录复核及告知情况
法律研究和内部知识管理	归纳资料、生成研究提纲、整理知识条目或培训材料	引用虚假或过时资料、错误内容进入知识库、来源和权利状态不清	核验规则、案例、数据和文献来源，确认引用和使用权限	记录主要来源、审核人员和知识内容更新时间

A.3 风险程度参考

- 下列因素可能提高人工智能使用风险：
- 输入信息包含客户保密信息、完整案件材料、敏感个人信息或者其他敏感法律业务信息；
 - 人工智能生成内容拟直接对外提交、交付或者用于作出业务决策；
 - 人工智能对事实认定、法律分析或者最终结论具有较高参与程度；
 - 事项涉及刑事责任、重大人身或者财产权益、重大交易、监管申报或者重大信息披露；
 - 错误内容难以及时发现、纠正或者可能造成不可逆的不利影响；
 - 人工智能工具的来源、数据处理规则或者输出局限不清晰。
- 具有一项或者多项前述因素的，法律从业人员宜提高人工复核、审批和留痕程度；符合第 3.8 条所述情形的，按照高风险使用场景处理。

附录 B
(资料性)
人工智能工具使用前审查清单

B.1 使用说明

本附录提供人工智能工具使用前审查事项示例，用于帮助法律从业人员和相关组织实施第 5 章规定的工具选用与使用准备要求。

审查程度宜与拟处理的业务和信息风险相适应。仅处理公开信息或者从事低风险辅助性工作的，可进行简化审查；拟处理完整案件材料、客户材料或者其他敏感法律业务信息的，宜进行较为充分的审查并确认相应保护措施。

本清单不构成人工智能工具的技术认证或者产品质量评价。

B.2 审查事项

表 B.1 人工智能工具使用前审查清单

序号	审查事项	参考审查内容	审查结果
1	工具来源	工具名称、服务提供者和获取渠道是否明确，是否能够获取必要的服务说明和联系方式	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
2	使用目的	拟使用的功能是否适合具体法律业务，是否明确人工智能仅用于辅助性工作	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
3	功能和局限	是否了解工具的主要功能、适用范围、已知局限和可能产生虚假输出等风险	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
4	组织准入	所在组织是否允许使用该工具、账户和相应功能，是否存在禁止或者限制使用的场景	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
5	账户和权限	是否使用适当的组织账户或授权账户，是否具有身份识别、权限控制和必要的访问限制	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
6	输入信息范围	拟输入的信息是否为完成任务所必需，是否包含完整案件材料、客户材料或其他敏感法律业务信息	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
7	数据保存	输入信息、对话记录和生成内容是否保存，保存位置、期限和访问主体是否能够了解	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
8	数据使用	输入信息或者生成内容是否可能被用于模型训练、产品改进、共享或者其他目的，是否能够关闭或者限制相关用途	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
9	数据删除	是否提供对输入信息、对话记录和生成内容进行删除、清理或者到期处置的机制	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
10	数据流向	信息是否可能由第三方处理、境外访问或者跨境传输，相关安排是否符合适用要求	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
11	本地或私有环境	采用本地化、私有化部署或者本地文件访问方式时，数据是否仍可能发送至外部服务，访问范围、网络连接和权限是否受控	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
12	保密和合同条件	服务条款、保密约定和责任安排是否与职业义务、委托约定和所在组织要求相符	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
13	知识产权	输入内容和生成内容的使用条件、权利声明及第三方内容处理规则是否清晰	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
14	记录和审查	对重要或高风险业务，是否能够保留必要的使用、复核和审批记录	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认
15	异常处置	是否明确发现严重错误输出、信息泄露或其他异常时的停止使用、报告和补救方式	☐ 符合 ☐ 不符合 ☐ 不适用 ☐ 待确认

B.3 审查结果处理

存在“不符合”或者重要事项“待确认”的，宜结合拟处理业务和信息的风险判断是否可以使用。涉及下列情形之一的，在相关问题得到解决前，不宜使用该工具处理相关业务：

- 工具来源或者服务提供者无法合理识别；
- 数据处理规则不清晰且拟输入敏感法律业务信息；
- 工具或者处理环境不符合保密、委托约定或者所在组织要求；
- 无法对拟处理的完整案件材料、客户材料或者其他敏感信息实施必要的访问控制；
- 所在组织已经禁止使用该工具或者相关功能；
- 其他可能对客户权益或者法律服务质量造成重大不利影响的情形。

审查结果宜由使用人员或者相关组织按照业务风险予以记录。工具功能、服务条款、数据处理规则或者使用环境发生重大变化时，可重新进行审查。

附录 C
(资料性)
输入信息与输出内容复核清单

C.1 使用说明

本附录提供人工智能使用前的输入信息审查事项和生成内容使用前的复核事项示例，用于帮助法律从业人员实施第 6 章和第 8 章的相关要求。

清单可根据具体业务、风险程度和所在组织要求进行调整。低风险、内部辅助性使用可采用简化清单；重要或者高风险法律业务宜保留必要的审查和复核记录。

C.2 输入信息审查清单

表 C.1 输入信息审查清单

序号	审查事项	参考审查内容	审查结果
1	工具和环境	拟使用的工具、账户和处理环境是否经允许并适合处理相应信息	☐ 是 ☐ 否 ☐ 待确认
2	国家秘密等信息	是否包含国家秘密、工作秘密、依法不得公开或者依法禁止处理的信息	☐ 是 ☐ 否 ☐ 待确认
3	客户和案件信	是否包含客户保密信息、未公开案件信息、完整案卷或者其	☐ 是 ☐ 否 ☐ 待确认

	息	他受保密义务约束的材料	
4	商业秘密	是否包含商业秘密、未公开交易信息或者其他可能影响相关主体竞争利益的信息	☐ 是 ☐ 否 ☐ 待确认
5	个人信息	是否包含个人信息或者敏感个人信息，是否具有相应处理依据	☐ 是 ☐ 否 ☐ 待确认
6	第三方权利	是否包含受著作权、合同约定或者其他第三方权利限制的内容，是否具有使用依据	☐ 是 ☐ 否 ☐ 待确认
7	最小必要	拟输入的信息范围是否为完成任务所必需，是否能够删除与任务无关的内容	☐ 是 ☐ 否 ☐ 待确认
8	信息处理	是否能够通过摘要、删除、替换、脱敏或结构化提取等方式减少原始信息输入	☐ 是 ☐ 否 ☐ 不适用
9	完整材料使用	确需使用完整案件或客户材料时，是否已确认工具环境、访问权限及必要保护措施	☐ 是 ☐ 否 ☐ 不适用
10	委托和组织要求	输入行为是否符合委托约定、客户授权和所在组织的禁止或限制要求	☐ 是 ☐ 否 ☐ 待确认
11	后续处理	是否了解输入信息和对话记录的保存、共享、删除及可能的数据流向	☐ 是 ☐ 否 ☐ 待确认

发现拟输入的信息属于依法禁止处理的信息，或者工具和处理环境明显不符合保密要求的，不应继续输入。其他存在风险的事项，宜在采取删除、替换、脱敏、调整工具环境、取得必要授权或者其他适当措施后再行使用。

C.3 输出内容复核清单

表 C.2 输出内容复核清单

序号	审查事项	参考审查内容	审查结果
1	证据材料	对证据名称、内容、来源和证明目的的描述是否准确，是否存在虚构或错误归纳	☐ 通过 ☐ 需修改 ☐ 不适用
2	法律依据	文件名称、发布机关、条文、效力层级、有效状态和适用范围是否准确	☐ 通过 ☐ 需修改 ☐ 不适用
3	案例引用	案例是否真实，案号、法院、日期、审级、裁判结果和裁判要旨是否准确	☐ 通过 ☐ 需修改 ☐ 不适用
4	数据和文献	数据、统计结论和文献是否来源明确、能够查证且未被曲解	☐ 通过 ☐ 需修改 ☐ 不适用

5	法律关系和逻辑	法律关系识别是否正确，事实、规则、论证和结论之间是否一致	☐ 通过 ☐ 需修改 ☐ 不适用
6	完整性	是否遗漏重要事实、证据、限制条件、例外、程序风险或者反方观点	☐ 通过 ☐ 需修改 ☐ 不适用
7	具体适用性	内容是否符合具体事项、客户目标、程序阶段和成果用途	☐ 通过 ☐ 需修改 ☐ 不适用
8	偏差和不当内容	是否存在偏见、歧视、刻板印象、误导性或者明显不当的表述	☐ 通过 ☐ 需修改 ☐ 不适用
9	保密风险	是否包含不应披露的客户、案件、个人或者其他敏感法律业务信息	☐ 通过 ☐ 需修改 ☐ 不适用
10	知识产权	是否可能不当复制第三方内容，引用、署名和使用方式是否适当	☐ 通过 ☐ 需修改 ☐ 不适用
11	格式和身份信息	当事人名称、文书类型、签署主体、日期、附件和格式是否准确完整	☐ 通过 ☐ 需修改 ☐ 不适用
12	告知和授权	是否依法、依职业规范或者委托约定需要告知、授权或说明，相关程序是否完成	☐ 通过 ☐ 需修改 ☐ 不适用
13	最终确认	是否已完成必要修改，是否由对成果负责的法律从业人员作出最终确认	☐ 通过 ☐ 需修改 ☐ 不适用

C.4 复核结果处理

复核结果为“需修改”的，应对相关内容进行核验、修改、补充、删除或者重新生成，并再次确认。无法从可靠来源核实的事实、证据、法律依据、案例、数据或者文献，不应用于正式法律服务成果。

对重要或者高风险法律业务，宜记录复核人员、复核时间、主要问题和处理结果。复核记录本身包含敏感法律业务信息的，应按照第 10.2 条予以保护。

附录 D (资料性) 禁止及限制使用行为示例

D.1 使用说明

本附录通过典型情形说明第 6 章、第 8 章和第 9 章规定的使用边界。具体行为是否适当，仍需结合所使用工具和处理环境、信息性质、授权情况、业务目的及可能后果进行判断。

本附录中的处理建议仅用于说明可能采取的规范措施，不替代法律法规、职业规范、委托约定或者所在组织制度的具体要求。

D.2 典型情形

表 D.1 禁止及限制使用行为示例

序号	审查事项	参考审查内容	审查结果
1	法律从业人员因分析完整事实链确有必要，在经组织允许的本地化或私有化环境中处理完整案件材料，并采取账户权限和访问控制措施	不因使用完整材料而当然构成不当行为。应重点判断任务必要性、处理环境、授权和保护措施是否适当	确认使用目的、权限范围、数据流向和复核安排；按照业务风险保留必要记录
2	法律从业人员使用能够访问本地文件的人工智能工具，但未确认文件是否发送至外部服务以及工具的访问范围	存在较高信息泄露风险，在相关事项未确认前不宜处理敏感法律业务信息	核查网络连接、外部调用、文件访问权限和数据保存规则；必要时限制目录、关闭外部传输或改用受控环境
3	人工智能生成了名称、条文和内容看似完整但实际不存在的法律依据，法律从业人员未经核验即在法律意见书中引用	属于禁止行为，违反人工复核和真实陈述要求	立即核验并删除虚构引用；成果已经交付的，及时更正、说明并评估影响
4	人工智能提供了无法查证的案例，法律从业人员将其作为诉讼文书论据提交	属于禁止行为，可能损害程序诚信和法律服务质量	仅引用能够从可靠来源核验的案例；已经提交的，依适用程序及时采取更正或其他补救措施

5	法律从业人员使用人工智能生成合同初稿，经结合交易背景和客户要求进行逐条审查、修改后交付	属于一般允许的辅助使用，但法律从业人员仍对最终合同成果负责	保留必要的人工复核；重大交易可记录工具用途、关键修改和审批情况
6	法律从业人员将人工智能生成的法律意见未经审查直接发送给客户，并使客户认为其为正式法律意见	属于禁止行为，违反人工复核和客户权益保护要求	停止直接交付；由法律从业人员结合具体事实和法律依据完成实质复核，并根据需要向客户说明
7	法律从业人员使用人工智能生成虚假的聊天记录、录音、图像、签名或者其他材料，用于证明案件事实	属于禁止行为，可能同时违反证据规则、职业规范或者法律规定	不得制作、提交或传播；发现已经使用的，应立即停止并依法依规处置
8	人工智能对案件结果给出确定性预测，法律从业人员未结合证据、程序和司法实践即据此建议客户采取诉讼策略	属于不当依赖。人工智能分析不应成为策略制定的唯一依据	由承办人员独立分析，说明不确定性、证据限制和可能的不同结果
9	法律从业人员使用人工智能辅助起草客户回复，已核实客户事实、法律依据并完成修改，但未就	是否需要告知应结合人工智能是否产生实质影响、职业规范和委托约定判断，不宜一概认定违规	对仅有一般性辅助且无特别要求的，可按内部规则处理；产生实质影响或涉及约定事项的，履行相应告知或授权程序

	一般性文字辅助单独告知客户		
10	法律从业人员将含有第三方受保护内容的材料输入工具，并直接对外使用高度相似的生成内容，未核查使用权限和来源	可能产生知识产权或合同违约风险	核查输入和输出内容的权利基础、相似程度及引用要求；必要时修改、取得授权或停止使用
11	法律从业人员已经发现生成内容存在重大错误，但未告知客户，也未纠正已经交付的成果	属于禁止行为，可能扩大客户损失和法律服务风险	及时停止使用，核验影响，并采取更正、说明、撤回或其他必要补救措施
12	所在组织明确禁止特定人工智能工具处理案件材料，法律从业人员仍使用个人账户处理	属于禁止行为，违反工具准入、账户管理和组织要求	停止使用并按内部制度处置；确有业务需要的，应先履行工具评估和批准程序
13	法律从业人员保留完整提示内容和完整生成内容作为留痕，导致不必要地重复保存大量客户敏感信息	留痕范围超过必要程度，可能增加信息泄露风险	根据业务风险保留工具、用途、输入信息类别、复核和责任人员等必要信息；确需保存完整内容的，采取相应保护措施

D.3 判断要点

对未列入表 D.1 的人工智能使用行为，可重点考虑以下问题：

使用目的是否属于法律业务中的合理辅助用途；

- 工具、账户和处理环境是否经允许且与信息敏感程度相适应；
- 输入信息是否具有合法、正当的处理基础并控制在必要范围；
- 是否由法律从业人员完成与风险相适应的人工复核和最终判断；
- 是否损害客户、当事人或者其他相关方合法权益；
- 是否存在伪造、误导、规避监管、逃避责任或者其他违反职业伦理的情形；
- 是否按照业务风险履行必要的告知、审批和留痕要求。

附录 E
(规范性)
分层培训课程与考核要求

E.1 一般要求

培训实施方应按照第 11 章和本附录确定培训课程和考核方案。培训层级应根据法律从业人员的岗位职责和人工智能使用场景确定。

各层级培训应以人工智能规范使用、风险识别、人工复核和必要操作为核心。培训实施方可根据不同法律职业和业务领域增加课程内容，但不应削减表 E.1 所列核心内容和考核要求。

E.2 分层培训要求

表 E.1 分层培训课程与考核要求

培训层级	主要培训对象	培训目标	核心课程内容	实践要求	考核要求
基础级	拟在法律服务、法律管理或法律研究工作中接触、使用人工智能工具的法律从业人员	理解人工智能的基本功能和局限，掌握规范使用底线，能够识别明显风险和禁止行为	人工智能基本特征和局限；常见虚假输出风险；保密义务；输入信息底线；最小必要；基本人工复核；客户权益；禁止行为；个人责任	应至少安排输入信息判断或者风险情境练习	应采用知识测试和情境判断；受训人员应能够识别不宜输入的信息、明显不可信的输出和禁止使用行为
应用级	经常在法律检索、案例分析、合同审查、文书起草、尽职	能够判断工具和任务是否适合，规范处理输入信息，核验生成内容并	工具和任务适用性；输入信息识别和保护；主要业务场景边界；事实、法律依据、案例、逻辑和完整性核验；成果修改和交	应安排至少一项与法律业务有关的综合场景实操，包含输入判断和输	应采用知识测试、案例判断和场景实操；受训人员应说明采用、修改或不采用生成内容的依据

	调查、合规管理、法律咨询等场景使用人工智能的法律从业人员	形成可交付成果	付：客户告知；使用留痕；风险事件处置	出复核	
管理级	在相关组织中承担人工智能使用管理、业务审核、风险控制、内部监督或培训组织职责的法律从业人员	能够建立和执行与业务风险相适应的使用控制措施，并组织处理违规或风险事件	工具准入；账户和权限；使用范围；场景风险控制；人工复核和审批；记录管理；监督检查；违规处理；风险事件处置；培训组织	应安排制度审查、管理方案设计或者风险事件处置练习	应采用案例分析、制度审查或管理方案设计；参训人员应能够识别管理缺陷、提出控制措施并说明处置依据
专家级	参与使用规范制定、重大法律业务风险审查、复杂事件调查、培训课程设计或相关标准建设的法律从业人员	能够处理复杂使用风险，设计使用规范和培训方案，并对标准实施效果进行评价	高风险业务边界；疑难职业伦理；系统性风险评估；重大事件分析和复盘；使用规范设计；培训方案设计；标准实施评价	应安排复杂案例综合分析和规范或培训方案设计；承担培训工作的，还应安排试讲或模拟评审	应采用综合案例、方案成果和答辩等方式；参训人员应能够说明规则依据、风险判断、控制措施和实施评价方法

E.3 考核方案

培训实施方制定的考核方案应至少明确：

培训层级和考核对象；

考核内容和考核方式；

知识测试、案例判断、实践任务或者方案成果的评价要点；

合格条件；

评价人员及其职责；

考核结果记录和复核方式；

不合格人员的补训和再次考核安排。

考核内容应覆盖表 E.1 所列培训目标和核心课程内容。应用级、管理级和专家级考核不应仅采用知识测试。

E.4 考核结果

受训人员完成规定课程并达到考核方案确定的合格条件后，可认定其完成相应层级的使用规范培训。

培训结果仅证明受训人员在考核时完成相应层级培训并达到相关考核要求，不应表述为取得法律执业资格、法律专业能力等级或者综合人工智能技术能力等级。

考核结果存在弄虚作假、考核材料来源不明或者其他影响结果真实性的情形时，培训实施方不应作出合格认定；已经作出认定的，应按照培训管理规则处理。

E.5 学时与更新

培训实施方应根据培训目标、课程内容、培训方式、实践任务和培训对象的基础情况合理确定培训学时。学时完成情况不应作为培训合格的唯一依据。

人工智能工具、法律法规、职业规范或者岗位职责发生重大变化，原有培训内容不能满足规范使用需要时，相关组织或者培训实施方应及时更新课程，并根据需要组织专项培训、补充培训或者重新考核。

参考文献

- [1] 《中华人民共和国律师法》
- [2] 《中华人民共和国公证法》
- [3] 《中华人民共和国仲裁法》
- [4] 《中华人民共和国网络安全法》
- [5] 《中华人民共和国数据安全法》
- [6] 《中华人民共和国个人信息保护法》
- [7] 《中华人民共和国保守国家秘密法》
- [8] 《中华人民共和国著作权法》
- [9] 《生成式人工智能服务管理暂行办法》
- [10] GB/T 41867—2022 《信息技术 人工智能 术语》

[11] T/AHA 010—2024 《法律大模型开发与应用服务规范》