

资料下载 / VERSION 1.0 / 2026-07-21

法律 AI 工具使用 安全自查清单（公开版）

一份供律师、法务及法律科技实践者在使用生成式 AI 前、使用中和对外发布前逐项勾选的基础检查表。

使用方法

每次处理新一批法律材料、新增一个 AI

服务或发布一份对外成果时，逐项勾选。任一红线项无法确认，先暂停上传、输出或发布，转人工复核。

01

材料进入 AI 之前

- ☐ 已确认材料的来源、使用目的与处理授权，不因“只做测试”而跳过保密义务。
- ☐ 已识别姓名、证件号、电话、账号、地址、案号、签名和其他可识别信息。
- ☐ 能用虚构主体、合成数据或最小必要片段完成的，不上传完整真实文件。
- ☐ 原始文件保持只读和可回溯；脱敏副本、输入版与对外版分开保存。

02

选择工具与设定边界

- ☐ 已核对服务商对输入数据的保留期限、训练用途、删除方式、存储地点和管理员可见范围。
- ☐ 涉及客户秘密、未公开案件材料或内部经营数据时，优先本地、私有化或经确认的企业环境。
- ☐ 已关闭非必要的共享链接、插件、第三方连接器和自动同步，并设置最小权限。
- ☐ 已记录当次使用的工具、版本、模型、日期与数据边界，便于事后复核。

03

对 AI 输出做专业复核

- ☐ 法条、案例、司法解释、机构名称、数字与引语均回到原始来源核对，不直接相信模型引用。
- ☐ 已区分“原文事实”“AI 推断”和“人工判断”，重要结论有可追溯依据。
- ☐ 已检查法律与政策的时效性、地域和适用条件，旧模型记忆不代表现行规则。
- ☐ 最终文书、建议或流程决定由有责任的人确认，AI 不单独决定责任边界。

从可复核流程到对外发布

04 让自动化可停止、可回读

- ☐ 对字段缺失、来源冲突、低置信度、目录不唯一等情形设置停止条件，不默认“猜一个结果”。
- ☐ 涉及发送、提交、删除、覆盖、公开发布等高影响动作时，保留人工确认节点。
- ☐ 流程完成后已在真实目标端回读，而非仅依据“任务成功”提示判断。
- ☐ 关键操作保留时间、输入来源、输出位置、校验结果和人工确认记录。

05 对外发送或公开发布之前

- ☐ 已检查正文、注释、批注、修订记录、文档属性、文件名、隐藏图层与可恢复内容。
- ☐ 已使用公开可验证来源，避免无授权复制第三方文章、图片、模板或数据库内容。
- ☐ 已删除真实客户、案件、联系方式、本地路径、私有链接和内部系统细节。
- ☐ 已说明 AI 辅助、合成数据、时效性和“不构成具体法律意见”等必要边界。

出现任一情形，暂停并转人工复核

- 无法确认材料授权或处理目的
- 真实客户或案件信息即将进入未经确认的在线服务
- 输出包含无法找到原始来源的法条、案例、数字或引语
- 自动化将直接发送、提交、删除、覆盖或公开发布
- 无法在最终目标端重新查看、校验或追溯处理结果

每次处理的最终结论

本次结论	☐ 可继续 ☐ 补充脱敏 ☐ 补充核验 ☐ 暂停处理
复核人 / 日期	_____
备注	_____ _____