

AI工具安全使用与数据合规基础课纲公开版

面向政府、国企、企业新员工、职能人员、业务人员和AI工具使用人员，帮助建立网络安全意识、数据合规边界和AI工具安全使用习惯。

公开边界

本资料为公开版课纲，不包含客户名称、内部制度、真实数据或定制案例。

课程定位

- 这是一门面向组织级AI应用前置培训的安全合规基础课。
- 课程围绕账号、密码、终端、邮件、文件、数据和AI工具使用风险，帮助学员形成可执行的安全行为习惯。
- 适合与AI通识课、AI办公提效课、新员工入职培训、全员安全月、保密教育和AI使用规范宣贯组合使用。
- 公开版为通用课纲，不包含任何客户名称、内部制度、真实数据或定制案例。

适合对象

- 政府、事业单位、国企和大型企业中需要使用AI工具的干部、员工和业务骨干。
- 新员工、职能人员、业务人员、培训对象和内部AI推广人员。
- HR、培训负责人、信息化部门、安全合规部门，用于判断AI培训前是否需要增加安全边界模块。
- 企业内训师和AI讲师，用于把AI工具教学与数据安全提醒结合起来。

课程采购价值

- 降低员工因无意识操作造成的数据泄露、账号风险、邮件风险和文件传输风险。
- 把传统网络安全意识与AI时代的数据合规风险结合，更贴近当前办公场景。
- 帮助企业在推进AI培训前，先建立“哪些资料不能上传、哪些结果必须复核、哪些工具需要审批”的共同语言。
- 适合政府、国企、金融、大型集团等关注数据安全、保密和合规边界的客户。

课程目标

- 识别常见网络安全风险和日常办公安全隐患。
- 理解数据安全、商业秘密、个人信息保护和内部资料使用的基本要求。
- 掌握AI工具使用中的敏感信息、模型幻觉、内容审核和人工复核边界。
- 形成个人网络安全与AI工具使用自查清单。

- 为后续AI办公提效、业务场景共创、智能体和知识库建设建立安全前提。

课程模块

- 模块1：网络安全底线。讲解账号密码、终端设备、邮件附件、文件传输、移动办公和外部协作中的常见风险。
- 模块2：常见攻击与案例。介绍钓鱼邮件、社工攻击、弱口令、恶意链接、公共Wi-Fi、假冒通知等常见攻击方式。
- 模块3：数据安全与保密。讲清客户信息、经营数据、技术资料、内部文件、会议纪要和项目材料的使用边界。
- 模块4：AI时代新风险。说明敏感信息上传外部AI、模型幻觉、生成内容外发、影子AI工具、账号共享和自动化工具权限滥用等风险。
- 模块5：个人行动清单。把安全要求转化为密码管理、文件处理、邮件识别、AI使用、异常上报和人工复核等日常行为。

AI工具安全使用边界

- 不上传涉密文件、客户数据、个人隐私、合同、经营数据、未公开方案和内部会议纪要。
- 需要使用真实业务材料时，先做脱敏处理，并确认是否允许使用外部工具。
- AI生成内容不得直接外发，涉及事实、政策、数据、法律、财务、客户承诺时必须人工复核。
- 不要共用个人账号处理组织资料，不要把AI账号、自动化工具和内部系统权限混用。
- 能用模拟材料讲清方法时，不用真实敏感材料演示。
- 对外发布内容要注意版权、肖像、商标、虚假宣传和夸大表达风险。

课堂练习建议

- 钓鱼邮件识别：从发件人、链接、附件、语气、异常要求和时间压力识别风险。
- 数据分类练习：区分公开资料、内部资料、敏感信息、客户信息和禁止上传信息。
- AI提示词改写：把包含敏感信息的原始需求改写为脱敏版本。
- AI输出复核：识别一段AI生成内容中的事实错误、夸大表达和需要引用来源的部分。
- 个人自查清单：让学员写出自己未来使用AI前必须检查的三条规则。

建议交付物

- AI工具安全使用清单。
- 员工网络安全行为自查表。
- 常见风险案例卡。
- 敏感信息脱敏示例。
- AI输出人工复核检查表。

- 适合后续接入AI培训或智能体建设的数据边界建议。

课前准备建议

- 确认参训对象：新员工、全员、业务骨干、管理者或AI推广人员。
- 确认单位是否已有AI工具使用规范、数据分级制度、保密要求或内部审批流程。
- 提前收集5到8个学员关心的问题，用通用化、脱敏化方式改造成课堂案例。
- 确认课程时长：半天版重点讲认知和清单，1天版可增加分组练习和岗位场景共创。

常见问题

AI培训前一定要讲数据安全边界吗？

建议讲。尤其是政府、国企、金融和大型企业，学员如果不知道哪些资料不能上传外部AI，后续应用越积极，风险越大。

这门课是网络安全课还是AI课？

它是网络安全意识与AI工具安全使用的结合课。重点不是技术攻防，而是让普通员工知道日常办公和使用AI时哪些行为有风险。

可以用企业真实资料做课堂练习吗？

可以，但必须先确认授权、脱敏规则、工具环境和使用边界。公开课和不确定环境下建议使用模拟材料。

AI生成内容为什么不能直接外发？

AI可能出现事实错误、引用不清、语气不当、版权风险或夸大表达。涉及对外沟通、客户承诺、政策数据和管理决策时必须人工复核。

这门课后续可以衔接什么服务？

可以衔接AI办公提效培训、企业AI使用规范、部门场景共创、知识库建设、智能体原型和内部AI讲师培养。