ChatGPT 如何赋能办公前沿实践

大数据与人工智能实战专家—李家贵老师

广东省人工智能与大数据中心技术总监/数据中台部总经理/CDO

课程背景：

本课程旨在探讨 ChatGPT 在信息安全领域所面临的挑战和问题，以及如何保护用户的个人信息和数据安全。随着 ChatGPT 等人工智能技术的广泛应用，信息安全和数据安全问题变得尤为重要。了解 ChatGPT 的安全问题，以及相关的信息安全和数据安全措施，对于保护个人和组织的利益至关重要。

课程特色：

综合性：本课程将综合考虑信息安全、数据安全和 ChatGPT 的安全问题，从多个角度全面探讨相关主题。

实践导向：除了理论知识，课程还将关注实际案例和解决方案，帮助学习者应对实际安全挑战。

细致深入：课程将深入研究 ChatGPT 的安全风险，包括个人信息保护、用户泄露事故和数据跨境安全等问题。

课程目标：

理解 ChatGPT 的先进性：学习 ChatGPT 的先进特征、提升原因和领域，认识到其在改变世界和影响社会的潜力。

了解信息安全和数据安全的基本概念：掌握信息安全和数据安全的基本原理、法律法规和最佳实践，理解其在保护个人和组织利益中的重要性。

分析 ChatGPT 的安全问题：深入研究 ChatGPT 的安全挑战，包括个人信息保护、用户泄露事故和数据跨境安全等问题，掌握相应的应对策略。

掌握信息安全和数据安全的管理方法：学习信息安全管理体系的建立和数据安全治理的基本过程，了解如何对信息和数据进行分级管理和全生命周期管控。

提高安全意识和应对能力：通过案例分析和讨论，培养学习者的安全意识，提高其在面对 ChatGPT 和相关安全问题时的应对能力。

授课形式：

案例分析、课堂讨论和互动答疑相结合。

课程时长：0.5 天。

课程大纲：

一、ChatGPT 改变世界

1.1 宏观认知

1.1.1 二季度政治局会议关于 chatGPT 会议结论的政策解读

1.1.2 人工智能的 iphone 时刻/登火箭时不要问坐那个座位

1.1.3 AI 的影响可能是反人性的

1.1.4 chatGPT 的影响可能是文艺复兴级的

1.1.5 新的大国竞争和 wintel 联盟

1.1.6 上一轮人工智能进入尾声

案例：5000 万美金的朋友圈

1.2 ChatGPT 的先进性

1.2.1 ChatGPT 具备诸多先进性特征

1.2.2 ChatGPT 提升的核心点

1.2.3 ChatGPT 提升的原因

1.2.4 ChatGPT 提升的领域

1.2.5 ChatGPT 得益于通用（基础）模型所构建 AI 系统的新范式

1.3 ChatGPT 的局限性

1.3.1 机器幻觉

1.3.2 知识库问题

1.3.3 信息安全

1.3.4 跨境传输

二、信息安全和数据安全

2.1 信息安全概述

驱动力：实施 ISO27001 的收益

信息安全管理精髓：基于风险管理的持续改进机制

管理体系融合思路

实施思路示例：信息与信息资产分级管理

实施思路示例：生产数据生命周期管理

多层级、针对性、全员开展的安全培训

2.2 数据安全概述

数据安全相关法律法规

依据:欧盟《通用数据保护条例》GDPR 合规指南

依据：网络安全法

等级保护制度 2.0 征求意见稿，数据安全相关解读

以数据为中心的安全建设理念

数据安全治理基本过程

数据分类及分级

对公司数据分级分类

数据全生命周期安全管控

数据安全分级分类

数据全生命周期管控（文档）

数据安全分级分类

服务器区数据安全解决方案