湖北省第二届“数字工匠”职工技能大赛

数据安全管理员赛项技术文件

2025 年 7 月

目 录

一、命题原则

依据国家职业技能标准，面向从事数据安全工作的职工，考核选手在数据安全法规、数据安全技术应用、人工智能安全应用、数据安全攻防对抗以及前沿技术与新兴威胁等方面的综合能力，旨在提升人工智能时代下的数据安全保障水平。

二、比赛形式

本赛项为个人赛，赛事设计对应全国总工会第二届职工数字化应用技术技能大赛数据安全管理员赛项的四个科目：理论考试、数据安全技能赛、数据安全综合场景赛、人工智能模型数据安全挑战赛等竞赛内容。其中，将人工智能模型数据安全挑战赛对应内容融合到数据安全技能赛和综合场景赛中。

省赛共计三场：数据安全理论赛、数据安全技能赛、数据安全综合场景赛。

三、比赛内容

竞赛内容共三场，第一场竞赛为理论竞赛、第二场为技能实操赛、第三场竞赛为综合场景赛。其中第一场和第二场竞赛在同时间段进行，三场比赛的成绩权重设定为 3（数据安全理论）：3（数据安全技能）：4（数据安全综合场景），所有场次竞赛均采用线下集中方式进行。

（一）第一场：数据安全理论赛（30%）

本场比赛总分 300 分，比赛时长 1 小时，模式为数据安全理论赛，理论试题根据选手 ID 从系统题库中随机生成。理论考点主要包括数据安全的政策法规标准以及技术知识点。

（二）第二场：数据安全技能赛（30%）

本场比赛总分 300 分，比赛时长 3 小时，模式为数据安全技能赛，数据安全技能赛分为数据安全题、数据分析题和模型安全题。知识点主要包括 API 接口安全、数据注入、数据高频采集、数据加解密、敏感数据识别、数据分类分级、数据脱敏、逆向分析、数据溯源与处置、模型数据安全等。

（三）第三场：数据安全综合场景赛（40%）

本场比赛总分 400 分，共计 4 小时，模式为数据安全综合场景赛。通过虚拟仿真企事业单位真实网络环境、重要数据业务系统、人工智能模型的全流程业务场景及面临的典型数据安全攻击事件，考察选手对于企事业单位综合业务场景下的数据安全应用防护与研判分析能力、人工智能模型应用与数据安全分析能力。涉及的知识点有：数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、数据溯源与处置、逆向分析、人工智能模型数据安全与应用等。

（四）实际操作

1.请使用 Firefox 或者 Chrome 浏览器访问竞赛平台，其他浏览器暂不兼容，可能会导致页面错位，无法提交 Flag 值。

2.使用浏览器访问竞赛平台时，请勿给浏览器设置代理，否则 Flag 将无法提交验证。

3.理论答题每一道题一次作答机会，提交答案后不可更改答案，可以先跳过不答，每道理论题都需要提交答案进行验证判分。

4.严禁利用扫描器对竞赛平台进行恶意扫描、或对竞赛平台发起 DDoS 攻击。一经发现即刻封锁账号，取消参赛资格。

5.请勿利用手机、互联网相互通讯，禁止交流讨论，协同作答。

6.如果对竞赛平台有疑问，或者对考题有疑义，或者其它与竞赛相关的事宜，请举手示意，切勿大声呼喊。

四、比赛规则

（一）第一场竞赛

采用竞赛系统在线答题，数据安全理论赛题型包括单选题、多选题、判断题，参赛选手需根据题目描述，选择合适选项进行作答，选手需逐题点击提交，提交之后无法修改答案。

（二）第二场竞赛

数据安全技能赛设置数据安全题、数据分析题和模型安全题三种题型，数据安全题预设指定“字符串”作为答案标识，选手通过各种技术手段分析获取答案，将答案提交至平台输入框即可，答对加分，答错不扣分；数据分析题采用大题小问形式，平台提供场景描述及题干要求，选手通过各种技术手段分析获取答案，将答案提交至平台对应题干下的输入框即可，答对加分，答错不扣分，限制答案提交次数为 10 次；模型安全题选手通过分析场景描述及要求完成解题，提交题干要求的附件至平台，选手主动点击题干下方的“提交答案”按钮选择对应需要提交的文件至平台，平台会自动进行答案验证，验证通过即可得分，验证不通过不扣分，平台限制验证次数为 10 次，系统实时统计分数并进行成绩展示。

（三）第三场竞赛

采用竞赛系统在线答题，竞赛平台将展示各参赛选手的 IP 地址段，考生需自己识别考题的网络拓扑结构，以便根据实际的场景进行题目作答，选手根据竞赛平台提供的题干描述以及提示进行答题，通过各种技术手段分析获取题干要求的答案，若答案格式要求为特定“字符串”标识，将“字符串”作为答案提交至平台输入框即可完成答题；若答案格式要求为特定“附件”，选手主动点击题干下方的“提交答案”按钮选择对应需要提交的文件至平台，平台会自动进行答案验证，验证通过即可得分，验证不通过不扣分，每道题

限制为 10 次答题机会，系统实时统计分数并进行成绩展示。

五、评分标准

选手个人总成绩=数据安全理论赛得分+数据安全技能赛得分+数据安全综合场景赛得分，竞赛排名按积分进行排序，总分相同，答题时间短的排名在前。

六、竞赛平台

图：竞赛平台登录页面

图：数据安全理论赛答题页面

图：数据安全技能赛答题页面

图：数据安全综合场景赛答题页面

图：人工智能模型数据安全挑战赛答题页面

图：竞赛实时展示成绩页面主界面

图：竞赛实时展示成绩页面英雄榜界面

图：竞赛实时展示成绩页面主界面数据分析界面

七、样题

（一）数据安全理论赛题

1.【单选题】数据脱敏（Data Masking）与数据匿名化（Data Anonymization）的根本区别是？

A. 脱敏可逆，匿名化不可逆

B. 脱敏用于结构化数据，匿名化用于非结构化数据

C. 脱敏保留数据关联性，匿名化完全破坏关联性

D. 两者为同一技术的不同名称

答案：A

解析：脱敏可能通过替换/扰动保留部分信息（如格式保留加密），而匿名化要求无法关联到个体。

2.【多选题】差分隐私的实现需要以下哪些关键参数？

A. 隐私预算 ε（Epsilon）

B. 敏感度（Sensitivity）

C. 加密密钥长度

D. 噪声机制（如拉普拉斯噪声）

答案：A、B、D

解析：ε 控制隐私保护强度，敏感度决定噪声量，噪声机制是核心实现方式。

3.【判断题】对抗样本攻击仅对计算机视觉模型有效，不影响自然语言处理模型。

答案：错误

解析：对抗样本可攻击任何类型的 AI 模型，包括 NLP 和语音模型。

（二）数据安全技能赛题

在竞赛系统中，屏幕左侧将呈现数据安全技能赛中“数据安全题”、“数据分析题”、“模型安全题”三个题型的选项卡。参赛者任意选定其中某个选项卡，即可清晰地看到对应题型下的题目数量及其对应的编号。参赛者有权根据个人意愿选择任意题目进行答题，无需遵循特定的先后顺序。

1. 数据安全题

图 1：数据安全题样题

2. 数据分析题

1) 题目背景

在现代社会，个人信息在各种场景下被持续采集和存储，形成了庞大的数据集合。随着这些数据的不断积累和汇聚，数据安全的重要性愈发凸显。如果缺乏有效的安全措施，敏感信息可能面临泄露、篡改甚至恶意滥用的风险，从而导致个人隐私遭受严重侵害，甚至引发更广泛的安全问题。因此，必须加强数据保护机制，确保信息在存储、传输和使用过程中得到严格的安全管控，以防止个人敏感数据的全面失控，保障公民的隐私权和信息安全。

下列数据样本源自暗网泄露数据，由多家企业的数据泄露事件以及网络爬虫汇总而成，请基于这些泄露数据，查找`张华强`的居住地和工作地名称、所属公司、手机号码、身份证号码及车牌号码。

2) 考题题干

任务一：张华强的居住地和工作地名称？

提示信息：

*工作地方一般为：**园区、 **大厦、**大楼*

涉及的经纬度信息均不考虑转换

张某的生活习惯为：周一到周五从家打车去公司，周末无明显固定作息

被泄露方验证泄露的数据，确定了泄露日期的真实性，行程的时间具体时间被隐去

答案提交:

将“张华强”的居住地和工作地的名称，用英文冒号(`:`)拼接后提交。如居住地为华侨小区 A 区，工作地为新东方创业园，则提交的答案为：华侨小区 A 区:新东方创业园

3. 模型安全题

图 2：模型安全题样题

1) 背景

随着人工智能技术的日益普及，其安全风险也逐渐凸显。在线零售平台广泛应用人工智能模型以提升运营效率和用户体验，例如情感分析模型被用于处理海量用户评论，辅助智能客服、商品推荐、舆情监控和供应链优化等关键业务环节。然而，这些模型面临着对抗样本攻击和模型投毒训练

攻击的 数据安全威胁。模型一旦遭受攻击或数据污染，可能导致业务中断、用户信任危机，甚至造成经济损失和运营混乱。因此，评估和提升人工智能模型的数据安全性，对于保障平台的健康发展和用户权益至关重要。

2) 场景描述

请选手作为一家在线零售服装平台的安全研究员，负责评估和提升平台商品评论情感分析模型的安全性。该模型用于自动识别用户对服装商品评论的情感倾向（正面/负面），直接影响商品推荐、舆情监控等关键业务。本次竞赛，您将模拟真实攻击场景，深入研究模型对抗样本攻击和模型投毒训练攻击两种关键的安全威胁，旨在全面检验和提升在线零售服装平台情感分析模型的安全防线，并为提 升模型鲁棒性提供技术方案。

（三）数据安全综合场景赛题

选手需自己识别赛题的网络拓扑结构，以便根据实际的场景进行题目作答，选手根据竞赛平台提供的题干描述以及提示进行答题。

1.场景说明

在这个场景中，某公司需要对三个系统进行全面的数据安全评估。参赛团队应从数据安全的角度出发，系统性地分析数据在整个生命周期中的各个环节，包括采集、传输、存储、利用、共享和销毁等。

2.场景拓扑

当前数据安全综合场景的模拟拓扑如下：

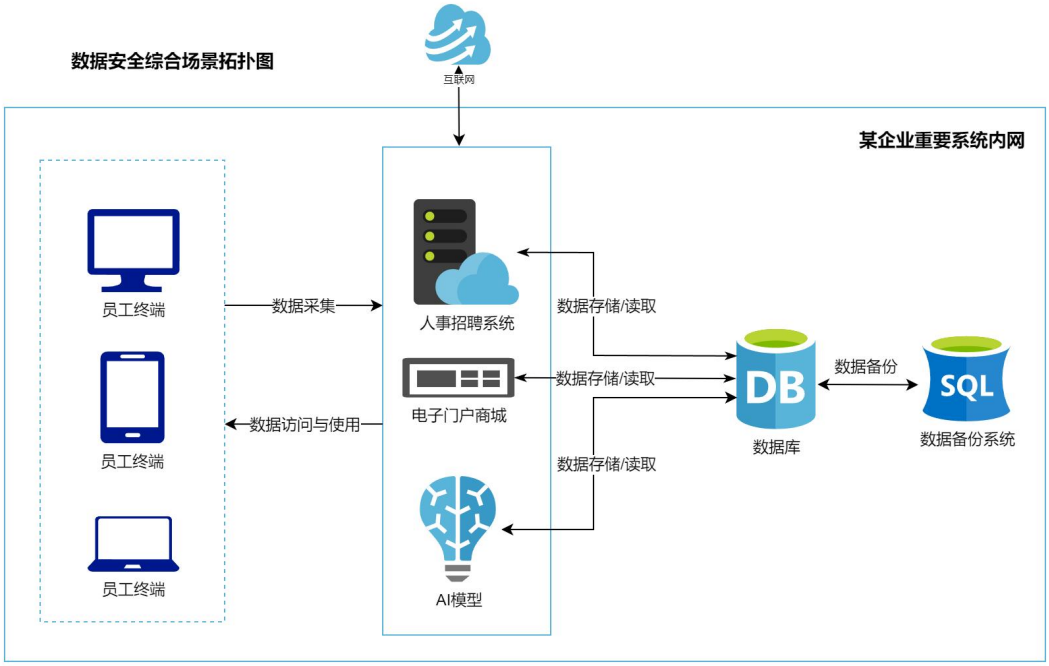

图 3：场景拓扑示例

3.场景题干

- **场景一：数据采集安全**

考题 1：请选手通过数据安全评估手段分析人事招聘系统，现有一批职业数据遭受了内部员工泄漏，好在人事招聘系统使用了数字水印技术，请你根据水印统计内部各个员工泄漏的图片数量，并从大到小进行排序。（访问人事招聘系统的/upload/watermark/水印.zip 下载附件）

【答案标准】例：若最终统计结果张三 100 张，李四 200 张，则最终提交答案为：李四-200,张三-100。

考题 2：.....

- **场景二：数据传输安全**

考题 1：请选手通过数据安全评估手段分析人事招聘系统,人事招聘系统同时向四位领导发送了同一批员工的联系方式。为了保护这些敏感数据，系统使用 RSA 算法对信息进行了加密。然而，在传输过程中，数据遭到了截获。现在，请根据给定的流量包(user.pcapng)和数据库 qs_boss 表信息还原这些联系方式的明文并将侯秀华的手机号作为答案提交。

【答案标准】例：若侯秀华的手机号为 13812345678，则最终答案为：13812345678。

考题 2：.....

- **场景三：数据存储安全**

考题 1：请选手通过数据安全评估手段分析人事招聘系统，找到被加密的核心配置文件，并根据网站环境配置，恢复其源码并将源码中存在的 flag 作为答案提交。

【答案标准】例：若获取的 flag 内容为：flag{ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c}。则提交最终答案为：ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c。

考题 2：.....

- **场景四：数据提供安全**

……

八、其他事项

（一）考试大纲：

1.政策法规和标准体系

掌握《中华人民共和国数据安全法》核心要求：数据分类分级制度、数据安全责任主体、数据安全风险评估与应急处置义务；

熟悉《中华人民共和国个人信息保护法》关键条款：最小必要原则、告知同意规则、个人信息跨境提供的安全评估要求、敏感个人信息处理限制；

了解《网络安全法》中与数据安全关联的内容；

掌握《关键信息基础设施安全保护条例》中涉及数据安全的要求；

熟悉《数据安全法》配套法规（如《数据出境安全评估办法》《个人信息出境标准合同办法》）的具体实施要求。

掌握国家标准：GB/T 43697-2024《数据安全技术 数据分类分级规则》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型（DSMM）》等内容；

熟悉行业标准：金融行业《金融数据安全 数据安全分级指南》（JR/T 0197-2020）、医疗行业《卫生信息安全等

级保护管理办法》等内容；

了解国际标准：ISO/IEC 27001（信息安全管理体系）、ISO/IEC 27701（隐私信息管理体系）、NIST SP 800-64（数据安全生命周期管理）、GDPR（欧盟通用数据保护条例）核心要求。

2.数据安全全生命周期管理

① 数据采集阶段

掌握合规采集原则、熟悉采集风险点、能识别违规采集行为，掌握采集安全技术等。

② 数据传输阶段

熟悉传输风险、掌握传输安全技术、了解传输安全工具。

③ 数据存储阶段

掌握存储风险、熟悉存储安全技术、了解存储介质安全。

④ 数据使用阶段

掌握使用风险、熟悉使用安全技术、了解使用场景安全。

⑤ 数据共享与销毁阶段

掌握共享风险、熟悉共享安全技术、掌握销毁风险、熟悉销毁安全技术。

3.数据安全核心的技术

掌握分类分级方法、熟悉分类分级工具、能结合行业标准完成数据分类分级实战；

掌握静态脱敏、动态脱敏技术，熟悉匿名化技术，能评

估脱敏效果；

掌握加密技术：对称加密（AES、SM4）、非对称加密（RSA、SM2）、同态加密（全同态/部分同态），熟悉隐私计算技术：

掌握 DLP 核心技术、熟悉 DLP 工具部署、能分析 DLP 误报/漏报场景。

4.人工智能安全技术基础

熟悉机器学习（监督/无监督/强化学习）、深度学习（CNN、RNN、Transformer）的核心原理与安全风险点；

掌握隐私计算技术（联邦学习、安全多方计算、同态加密）在 AI 中的应用场景（如跨机构联合建模、敏感数据协同分析）；

了解 AI 伦理与安全的关系（如算法偏见导致的歧视性决策、生成式 AI 的虚假信息传播风险）。

5.人工智能安全技术核心

握对抗样本攻击（白盒/黑盒）与防御（对抗训练、随机平滑）、模型鲁棒性评估；

熟悉训练数据清洗（异常值检测、重复数据删除）、隐私保护（差分隐私在 NLP/CV 中的应用）、模型输出脱敏；

掌握大模型提示注入攻击（Prompt Injection）、越狱攻击（Jailbreak）的检测与防御（如指令微调、内容过滤）；

熟练使用 AI 安全工具（对抗样本生成工具 Foolbox、模

型评估工具 IBM AIF360、隐私计算框架 FATE）。

6.其他

熟悉密码技术的概念、加密体制的分类、常见加密方式、密码协议与密码分析工具的利用；

熟悉物联网、工业控制、无线、网络设备等相关方面的安全问题；

熟悉移动互联网恶意程序监测与处置机制，掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等；

掌握常见协议分析工具的使用，常见数据包分析方法；

熟练使用数据恢复的常用技术等相关知识点内容；

熟悉恶意代码的识别方法及防护措施。能运用相关技术发现、隔离、清除常见恶意代码；并能对常见恶意代码进行逆向分析。

（二）竞赛纪律（线下决赛）

1.参赛队伍自行携带笔记本电脑、有线鼠标、RJ54 网口转接头、键盘和本人身份证原件进入赛场，提前准备相关知识库与工具；

2.参赛队伍在竞赛开始前 60 分钟签到，竞赛正式开始后迟到者（迟到 15 分钟及以上）将不得进入竞赛场地；

3.竞赛座位按照事先分派决定，正式竞赛期间参赛选手不得擅自离开竞赛座位，应举手请示工作人员，得到同意后

方可离开自己竞赛座位；

4.竞赛开始前选手先测试网络是否正常，是否能够正常访问比赛平台，如果无法正常访问比赛平台应及时举手等待现场工作人员帮助；

5.竞赛开始前选手手机一律上缴，由举办方暂时保管，比赛结束后有秩序地领回自己手机。上缴前需提前安排好自身工作，若因手机上缴而影响个人工作导致重大后果的，举办方一律不承担相关责任；竞赛过程中，如果发现选手将手机带入考场座位，按作弊处理。

6.竞赛过程中禁止选手接入互联网，禁止通过互联网查找资料，禁止通过任何形式寻求网络外援远程协助答题，发现违规者一律取消参赛资格；

7.比赛过程中禁止使用通用防御脚本/工具防御对手攻击，一旦被检测并查实使用通用防御则进行扣分并警告，经警告 3 次仍然不撤销通用防御队伍决赛记 0 分；

8.竞赛过程中或竞赛后如有任何问题（包括反映竞赛或其它问题），应立即举手示意，等待现场工作人员帮助；

9.比赛过程中，不同队伍之间不允许以任何形式相互讨论、交流、合作、分享资料，一经发现直接取消比赛资格，相关队伍立刻离场；

10.任何时候禁止攻击裁判服务器，否则将判令停止比赛，决赛分数为 0 分；

11 比赛过程中应遵守赛场秩序，禁止大声喧哗影响其他队伍比赛；

12.比赛过程中以及比赛结束后裁判有权抽查参赛选手解题方法/得分思路，如果发现回答有误，疑似通过作弊获得分数将对参赛选手扣分，严重者取消参赛资格；

13.裁判组将视情况对违反比赛纪律的行为采取禁赛、取消比赛成绩等处罚措施，情节严重者将在行业内通报。