ICS 35.020
CCS A 00

T/CCIASC

中 国 计 算 机 行 业 协 会 团 体 标 准

T/CCIASC XXXX—XXXX

网络和数据安全赛事平台建设规范

Specification of Network and Data Security Competition Platform Construction

（征求意见稿）

2025 年 12 月 8 日

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国计算机行业协会　　发 布

目　　次

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。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件起草单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国移动通信集团有限公司、中国联合网络通信集团有限公司、湖北省数字证书认证管理中心有限公司、江苏君立华域信息安全技术股份有限公司、永信至诚科技集团股份有限公司、南京赛宁信息技术有限公司、北京智游网安科技有限公司。

本文件主要起草人：王子卓、孟繁峻、杨军、秦晓磊、崔喻、宫文涛、房沛荣、温暖、周莹、周映、王晨旭、陈诚、张成群、陈楠、唐海均、张佳佳。

引　言

随着网络空间安全威胁日益复杂化、数据要素价值持续提升，国家对网络安全和数据安全领域的人才培养与能力验证提出更高要求。近年来，全国各级各类网络和数据安全赛事规模快速增长，但赛事平台建设缺乏统一规范，导致赛事公信力受损、参赛体验下降。

本文件基于《中华人民共和国网络安全法》《中华人民共和国数据安全法》及《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》等法规政策要求，针对行业痛点，系统规定网络和数据安全赛事平台的功能、安全性及可靠性要求，推动赛事平台从“基础功能可用”向“安全可信、数据驱动、人才赋能”的高质量发展转型。

网络和数据安全赛事平台建设规范

1 范围

本文件规定了网络和数据安全赛事平台建设的相关要求，有助于规范平台建设方的网络和数据安全赛事平台建设。

本文件适用于指导网络和数据安全赛事平台的开发企业、系统集成服务商等平台建设方建设功能全面、安全、可靠和稳定的网络和数据安全赛事平台。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 41479 信息安全技术 网络数据处理安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

注：引自GB/T 41479—2022，定义3.616

3.2

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

注：引自GB/T 41479—2022，定义3.4

3.3

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

注：个人信息包括姓名、出生日期、公民身份号码、个人生物特征信息、住址、联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注：个人信息控制者通过个人信息或其他加工处理后形成的信息，例如，用户画像特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，也属于个人信息。

注：引自GB/T 25069—2022，定义3.196

3.4

网络和数据安全赛事 network and data security competitions

指专门针对网络和数据安全领域举办的竞赛活动，旨在提升网络和数据安全技能、选拔优秀人才、促进网络和数据安全技术的发展和普及。这些赛事通常由政府机构、行业协会、科研机构或企业组织，覆盖网络安全、数据保护、数据治理等多个方面。

3.5

网络和数据安全赛事平台 network and data security competitions platform

指为网络和数据安全领域竞赛活动提供覆盖赛前准备、赛中执行、赛后分析全生命周期数字化支撑的综合性管理系统。

4 功能要求

4.1 人员管理功能要求

4.1.1 注册功能要求

a) 应建立标准化的注册流程，确保用户能够通过清晰指引完成注册操作，注册流程步骤应最小化，避免冗余环节；

b) 应要求用户提交真实、有效且完整的个人信息，包括但不限于姓名、有效身份证件号码、联系方式等必要字段；

c) 应采用多因素身份验证机制，在注册阶段实施必要的身份核验程序，验证方式应包含至少两种有效验证手段；

d) 应提供结构化使用条款和隐私政策文本，要求用户在注册前通过勾选确认已阅读并同意相关内容，确认过程应具备可追溯性；

e) 应建立数据安全防护体系，对注册信息采取加密存储、访问控制等技术措施，确保信息在传输和存储过程中的安全性；

f) 应建立注册审核机制，对异常注册行为进行风险评估，对不符合规范的申请应生成审核意见并提供补充材料指引；

g) 应通过邮件或短信等可靠渠道发送注册确认通知，通知内容应包含注册信息摘要及验证链接；

h) 应配备密码找回功能，支持通过安全问题验证、手机验证码、邮箱重置等方式实现账户恢复，相关操作应记录完整审计日志；

i) 宜支持多种注册方式，包括但不限于电子邮箱、手机号码等，每种注册方式应配置独立的验证通道；

j) 宜接入第三方账号授权接口，允许用户通过微信、QQ等主流社交平台实现快速注册，需明确标注授权范围及数据使用条款。

4.1.2 登录功能要求

a) 应提供直观、易用的登录界面，便于用户输入身份认证信息；

b) 应采用加密技术保障登录过程中的数据传输安全，防范中间人攻击；

c) 应设置连续失败登录次数限制，防止因频繁尝试导致的安全风险；

d) 应记录登录行为日志，包含成功与失败的登录事件，确保可追溯性；

e) 应通过安全机制实现密码重置与修改功能，保障账户信息安全；

f） 应配置会话超时策略，当用户无操作达到设定时间后自动终止会话；
g） 宜支持多种身份验证方式，包括但不限于用户名和密码、双因素认证、第三方账号授权等；
h） 可集成单点登录（SSO）功能，实现跨系统或服务的统一身份认证。

4.1.3 个人信息修改功能要求

a） 应提供用户友好的个人信息编辑界面，便于用户进行信息更新；
b） 应允许用户在不泄露敏感信息的前提下，对姓名、联系方式等基础信息进行编辑和更新；
c） 应在个人信息编辑过程中采取必要措施，保障用户隐私安全，防止未授权访问或信息泄露；
d） 应支持用户定期修改密码，并设置密码复杂度要求以提升账户安全性；
e） 应保证个人信息编辑功能在各类设备及浏览器环境下正常运行，实现用户体验的一致性；
f） 应建立必要的验证机制，对用户提交的个人信息变更请求进行审核，防范非法或不当修改；
g） 应记录所有个人信息变更的操作日志，确保可追溯性和审计需求；
h） 宜为用户提供撤销最近一次个人信息更改的功能，以降低误操作导致的信息错误风险；
i） 宜提供详细的帮助文档或在线客服支持，指导用户正确操作个人信息管理功能。

4.1.4 团队管理功能要求

a） 应具备团队成员角色分配与权限管理功能，明确不同角色的操作权限范围；
b） 应支持团队成员信息的录入、更新及查询功能，确保信息的准确性和时效性；
c） 宜配备团队协作工具，包括但不限于在线讨论区、文件共享等模块，提升团队内部沟通效率；
d） 宜建立团队活动记录与成果展示机制，强化团队协作成果的可视化呈现。

4.1.5 赛事裁判管理功能要求

a） 应建立裁判注册与认证体系，确保所有参与赛事的裁判具备法定资格和专业能力；
b） 应设立裁判申诉处理通道，明确异议提交流程、核查程序及处理时限，确保争议事项得到公正、透明的处置；
c） 应设置裁判资源调配模块，允许赛事组织方根据赛事类型、规模及需求，按层级或分类方式配置裁判团队，并支持临时调整机制；
d） 应采取技术防护措施，对裁判个人信息、工作数据等敏感内容实施分级权限管理，防止未经授权的访问、篡改或泄露；
e） 宜提供多模式沟通协作平台，支持裁判间在线讨论、文件共享、任务协同等功能，保障跨地域、跨时区的高效协作；
f） 宜配置裁判能力发展模块，包含标准化培训课程、模拟演练系统及定期考核机制，持续提升裁判的专业素养和技术水平；
g） 宜构建裁判信息数据库，支持对裁判个人信息、专业资质、历史执裁记录等数据的动态维护与更新，确保信息完整性和时效性；
h） 宜建立裁判绩效评估系统，通过量化指标记录裁判在各赛事中的工作表现，包括评分准确性、判罚一致性等关键维度，形成可追溯的评价档案。

4.1.6 消息通知功能要求

a） 应提供实时消息推送服务，确保赛事相关人员能够及时获取重要通知信息；
b） 应建立消息阅读状态反馈机制，通过已读和未读标识实现信息传递效果追踪；

c） 应具备消息记录存档功能，包含发送时间、内容及接收方状态等关键要素；
d） 宜具备批量消息发送能力，支持对特定群体或全量用户进行统一信息推送；
e） 宜支持自定义消息模板配置，可根据赛事阶段生成差异化通知内容；
f） 宜构建多通道消息传输体系，集成站内信、电子邮件、短信等主流通信方式；
g） 宜提供消息分类管理功能，允许用户按类型、优先级或主题设置信息过滤规则；
h） 宜设置消息优先级分级机制，对紧急事件信息实施特殊通道快速传达。

4.2 题目管理功能要求

4.2.1 题目设计功能要求

a） 应具备部署网络攻击与防御、漏洞利用与修复、密码学原理与应用、恶意软件分析与对抗等方向题目的能力；
b） 应支持部署选择题、填空题、简答题、案例分析题及实际操作题等多种类型的题目；
c） 应支持题目难度分级设置，覆盖基础至高级水平，满足不同参赛者的能力需求；
d） 应支持题目作者上传包含背景信息、问题描述、预期答案及评分标准的完整内容；
e） 应具备题目审核流程，确保题目内容准确无误且符合赛事规则；
f） 应具备题目数据统计分析功能，为赛事组织者提供难易度评估和参赛者表现分析依据；
g） 宜提供经典题目标签化存储功能，支持作为模板供后续题目开发使用；
h） 宜支持题目版本管理功能，便于对已发布题目进行更新或修正。

4.2.2 题目保密功能要求

a） 应采用加密技术对比赛题目的提交、存储及传输过程进行保护，确保数据在全生命周期内的机密性；
b） 应建立分级授权管理体系，通过角色权限配置实现对题目相关操作的最小权限控制；
c） 应具备全过程操作日志记录功能，包括但不限于题目创建、修改、发布、访问等关键操作，日志保存周期应满足审计追溯要求；
d） 应制定信息安全事件应急预案，明确题目泄露场景下的处置流程、责任分工及恢复措施；
e） 宜部署异常行为监测系统，通过流量分析、访问频次等指标识别潜在泄露风险；
f） 宜提供匿名化题目上传通道，通过脱敏处理实现身份信息与提交内容的隔离。

4.2.3 题目部署功能要求

a） 应具备自动化题目部署能力，确保题目在比赛环境中实现快速、精准的部署；
b） 应支持题目部署的版本控制机制，允许管理员回滚至历史版本；
c） 应具备题目部署数据的备份与恢复能力，确保比赛连续性及系统稳定性；
d） 应建立完整的部署日志记录体系，涵盖部署过程的关键操作与异常信息，满足故障排查与审计需求；
e） 应采用加密传输等技术手段保障题目数据在部署过程中的安全性，防止敏感信息泄露；
f） 应设置权限分级管理机制，明确不同角色对题目部署相关操作的访问与执行权限；
g） 宜提供题目部署状态的实时监控功能，及时发现并响应异常情况；
h） 宜根据比赛需求动态调整题目的难度等级与数量配置。

4.3 赛事管理功能要求

4.3.1 赛事信息发布功能要求

a） 应建立赛事信息展示系统，确保参赛者能够通过统一界面获取赛事基本信息、参赛须知及注意事项等核心内容，信息呈现应具备清晰性、准确性与完整性；

b） 应实现赛事数据实时更新机制，包括成绩录入、排名变动、奖项公示等动态信息，更新过程应保留操作日志并设置审核流程；

c） 应设置赛事日程管理系统，按时间轴形式展示比赛安排，包含具体时段、场地位置、赛程流程及关键节点说明，支持按项目或组别分类检索；

d） 应建立信息发布审核制度，确保发布内容符合法律法规和技术规范要求；

e） 应建立赛事文件库，支持规则手册、评分标准、技术规范等文档的上传、版本管理和权限控制，确保文件获取路径明确且访问便捷；

f） 应提供赛事资料归档服务，包含比赛录像、现场照片、技术报告等数字资源的存储、分类和检索功能，支持按时间、项目和人员等维度进行关联查询；

g） 应配置实时通知系统，通过站内消息、短信推送、邮件提醒等方式向注册用户发送重要变更信息，通知内容需包含变更事项、生效时间和影响范围；

h） 宜提供日程动态调整功能，允许赛事组织方在特殊情况下对既定安排进行修改，并同步更新至相关终端设备；

i） 宜采用分级存储策略，对公开文件与内部资料实施差异化管理，同时提供全文检索和下载记录追溯功能；

j） 宜建立公告分类体系，区分常规通知、紧急通告和政策解读等类型，支持历史公告的归档查询与多维度筛选；

k） 宜开发可视化数据看板，以图表形式展示赛事进程、参赛情况和结果统计等核心指标；

l） 宜构建多渠道信息分发机制，通过官方网站、移动应用、社交媒体平台等载体实现赛事信息的同步发布，扩大信息覆盖范围并提升传播效率；

m） 宜构建多媒体资源管理系统，实现音视频文件的转码处理、元数据标注及多格式输出，满足不同终端设备的播放需求。

4.3.2 赛事报名管理功能要求

a） 应建立报名审核机制，由赛事组织方对提交的报名材料进行资格审查，确保参赛人员符合相关条件；

b） 应支持多种支付方式，供参赛者缴纳报名费用，并应保障交易过程的安全性；

c） 应具备赛事通知功能，及时向已报名参赛者推送比赛时间、地点、规则调整等重要信息；

d） 应允许参赛者在规定时限内修改或取消报名申请，并应记录操作日志以备追溯；

e） 应确保报名数据的存储安全性，采取有效措施防止未授权访问、数据泄露或篡改；

f） 宜提供赛事报名统计功能，支持对报名数据的分类汇总与分析，辅助赛事组织方决策。

4.3.3 赛事流程管理功能要求

a） 应提供结构化赛事流程图，清晰展示报名、赛程安排、比赛执行、成绩统计及颁奖等核心阶段，并标注各阶段的关键时间节点；

b） 应具备赛事暂停与恢复操作权限，支持在不可抗力或突发状况下临时中止赛事，并提供恢复执行的流程指引及数据保存机制；

c） 应具备基于规则的任务自动分配功能，将赛事各阶段的工作任务（如裁判调度、场地准备、设备调试等）精准分派至对应责任人；

d） 应提供实时进度可视化界面，动态显示赛事当前所处阶段、关键节点完成状态及剩余时间，支持多维度数据展示（如时间轴、甘特图等）；

e） 应建立完整的操作日志体系，详细记录赛事流程变更、任务分配调整、人员操作行为等关键信息，确保可追溯性；

f） 宜通过系统通知、短信或邮件等方式，在关键节点前设定预警阈值，提前向相关人员发送工作准备提示；

g） 宜支持赛事流程模板的自定义配置功能，允许组织者根据赛事类型、规模及实际需求调整流程模块及顺序；

h） 宜构建突发事件处置预案库，支持快速触发预设应急方案，并通过多通道通知机制同步告警信息至相关责任人。

4.3.4 赛事监控控制功能要求

a） 应具备实时监控能力，对比赛过程中的各项活动进行持续监测，保障赛事运行安全与秩序；

b） 应设置权限管理机制，实现对监控数据访问和操作的分级授权管控；

c） 应建立异常检测机制，能够及时识别潜在安全风险及异常行为并触发预警；

d） 应配置事件响应功能，在检测到异常时能快速启动应急预案并执行处置措施；

e） 应具备日志记录功能，完整留存监控操作记录及结果数据，满足审计追溯需求；

f） 宜提供可视化监控界面，通过图形化方式呈现赛事状态信息和监控数据；

g） 宜支持多维度监控指标体系，涵盖参赛者行为、系统性能、网络安全状态等关键要素；

h） 宜支持远程监控功能，允许通过网络实现跨地域的实时赛事监控与管理。

4.4 成绩管理功能要求

4.4.1 成绩录入功能要求

a） 应提供用户友好的成绩录入界面，确保裁判便捷高效地完成参赛者成绩的录入工作；

b） 应支持多种成绩录入方式，包括手动输入、批量导入等，以提升操作灵活性；

c） 应建立成绩审核机制，确保录入成绩的准确性与评分标准的一致性；

d） 应允许裁判对已录入的成绩进行修改，并记录每次修改的日志。

4.4.2 成绩大屏功能要求

a） 应具备实时更新的成绩展示功能，确保大屏幕显示的比赛成绩与实际比赛结果一致；

b） 应允许赛事组织者选择需展示的具体成绩项，包括总分、单项得分、排名等；

c） 应提供多种可视化图表（如柱状图、折线图、饼图等），以直观形式呈现比赛成绩；

d） 应具备动态图表更新功能，当成绩发生变化时，图表能自动刷新以反映最新数据；

e） 应允许赛事组织者根据不同维度（如参赛者姓名、队伍名称、比赛阶段等）筛选和展示特定成绩信息；

f） 应设置严格的权限管理机制，仅授权人员可对大屏幕内容进行编辑和控制；

g） 应支持全屏模式，确保大屏幕内容清晰可见，便于观众观看；

h） 应确保成绩数据与后台数据库实时同步，避免信息不一致；

i） 宜允许赛事组织者自定义大屏幕布局，包括图表位置、大小及样式；

j） 宜提供简洁的导航按钮，方便用户在不同视图间切换；
k） 宜提供预设模板，供用户快速选择常用布局方案；
l） 宜记录所有对大屏幕内容的操作日志，便于追踪和审计；
m） 宜提供高级筛选选项，支持组合条件筛选，以便更精确地展示所需数据；
n） 宜支持紧急情况下的快速切换功能，允许在意外情况下迅速切换至备用显示内容；
o） 宜支持远程控制功能，允许赛事组织者通过网络从不同地点实时调整大屏幕内容。

4.4.3 成绩统计分析功能要求

a） 应具备自动化成绩统计功能，生成完整的参赛者成绩报告；
b） 应支持多维度的成绩分析，包括但不限于平均分、最高分、最低分及排名等指标；
c） 应提供可视化图表展示功能，便于赛事组织者直观掌握成绩分布情况；
d） 应允许用户根据需求导出成绩数据，满足后续分析或存档要求；
e） 应具备异常成绩检测机制，及时识别并处理异常数据。

4.5 解说管理功能要求

4.5.1 解说员注册功能要求

a） 应建立解说员注册机制，要求注册人员提交身份证明、专业资质证书及过往工作经历等基础信息，并通过平台资质审核；
b） 应对注册解说员实施分级管理，根据专业能力划分不同服务权限，并建立培训考核档案；
c） 宜设置解说员信息动态更新功能，允许其定期补充或修改个人资料、专业领域及服务记录；
d） 宜提供解说员信用评价体系，通过观众反馈、赛事管理员评分等方式形成综合评价数据。

4.5.2 解说任务分配功能要求

a） 应构建任务分配系统，支持赛事管理员按比赛阶段、项目类型、语言需求等维度匹配解说员；
b） 应允许赛事管理员手动调整任务分配，包括临时替换、增派支援及跨区域调度；
c） 应具备任务撤销与重新分配功能，应对突发情况时快速响应并记录变更原因。
d） 宜建立任务执行监控机制，实时跟踪解说员到岗情况及任务进度；
e） 宜实现任务自动分配算法，结合解说员历史表现、专业背景及空闲状态优化匹配效率；

4.5.3 解说内容管理功能要求

a） 应提供结构化解说内容编辑界面，支持文本、音视频、图文混排等多种格式的素材上传与编辑；
b） 应设置敏感词过滤机制，自动识别并标记可能引发争议或违规的内容；
c） 应建立三级审核流程：解说员自审、赛事管理员初审、专业审核团队终审，确保内容质量；
d） 应记录所有内容操作日志，包括编辑时间、修改人、版本差异及审批记录，保存期限不少于六个月；
e） 宜支持解说内容版本控制，允许回溯历史版本并生成对比报告；
f） 宜开发智能校验工具，对解说稿中的术语准确性、赛事规则合规性进行初步筛查。

4.5.4 解说互动功能要求

a） 应搭建多渠道互动平台，包含实时弹幕、问答专区、语音留言等交互形式，促进观众与解说员沟通；

b） 应建立互动数据归档制度，对重要对话记录进行加密存储，确保可追溯性；
c） 应具备互动内容实时审核功能，通过人工+AI双重机制过滤不当言论及广告信息；
d） 宜支持解说员创建专属互动话题，引导观众围绕赛事热点展开讨论；
e） 宜提供实时互动数据分析模块，统计观众参与度、热点问题及反馈趋势，辅助优化解说策略；
f） 宜开发互动效果评估体系，通过观众满意度调查、互动频次等指标量化分析互动质量。

4.6 防作弊功能要求

4.6.1 实时监测与行为分析功能要求

a） 应建立实时监测机制，通过算法模型对参赛者操作行为进行动态分析，识别高频提交、非正常答题路径等异常操作模式；
b） 应设置阈值预警规则，对疑似作弊行为触发分级告警，并生成包含操作轨迹、时间序列及关键指标的审计报告；
c） 宜采用多维度数据关联分析技术，结合时间戳、IP地址、设备指纹等信息，构建参赛者行为特征图谱；
d） 宜支持人工复核机制，允许赛事管理员对系统标记的可疑行为进行二次验证并记录处理结果。

4.6.2 技术防护与证据固化功能要求

a） 应部署防篡改技术，对比赛过程中的关键数据（如答题记录、评分结果）实施哈希校验与数字签名，确保数据完整性；
b） 应建立证据链管理模块，自动采集并固化可疑行为的原始数据，包括屏幕截图、操作日志及网络流量记录；
c） 宜采用加密存储与传输技术，对参赛者敏感信息（如身份标识、操作日志）进行端到端加密保护；
d） 宜配置区块链存证功能，将重要赛事数据上链存证，增强证据的不可篡改性与法律效力。

4.6.3 处理流程与责任追溯功能要求

a） 应具备标准化作弊处理流程，明确从发现、核实到处置的各环节责任人及操作规范；
b） 应记录完整的作弊事件处理日志，包括时间、操作人、处理依据及结果，并保留不少于三年的审计追溯周期；
c） 宜支持多级处罚机制，根据作弊严重程度采取警告、成绩扣减、取消资格等差异化处理措施；
d） 宜提供申诉通道，允许参赛者对作弊判定结果提出异议，并建立复核与反馈机制。

4.7 数据样本下载功能要求

4.7.1 数据分类与权限控制功能要求

a） 应按数据类型（如题目数据、成绩数据、行为日志）进行分类管理，明确不同类别数据的下载权限与使用范围；
b） 应支持数据脱敏处理，对涉及个人隐私或商业机密的信息（如身份证号、联系方式）进行匿名化或加密处理；
c） 宜设置分级访问策略，通过角色权限控制实现对敏感数据的最小化授权，防止未授权访问；
d） 宜提供数据使用协议签署功能，用户需在下载前确认遵守相关法律法规及数据使用条款。

4.7.2 下载格式与安全传输功能要求

a) 应支持多种数据格式导出（如CSV、Excel、JSON），满足不同分析场景需求；
b) 应限制单次下载数据量及频率，防止大规模数据泄露风险；
c) 宜采用加密传输技术（如HTTPS、SFTP），确保数据在下载过程中的安全性；
d) 宜配置下载记录审计功能，跟踪用户操作轨迹并生成可追溯的日志报告。

4.7.3 数据完整性与版本管理功能要求

a) 应保证下载数据的完整性，提供校验码（如MD5、SHA-256）供用户验证数据一致性；
b) 应建立数据更新通知机制，当数据源发生变更时及时向用户推送更新提示；
c) 宜支持历史版本回溯功能，允许用户根据时间或事件节点获取特定版本的数据集；
d) 宜提供数据质量评估指标（如缺失率、重复率），辅助用户判断数据可用性。

4.8 人才技能画像功能要求

4.8.1 多维度数据采集功能要求

a) 应整合参赛者多维度数据（如题目作答情况、成绩表现、行为特征、互动记录等），构建全面的能力评估基础；
b) 应动态更新数据标签，根据参赛者最新表现自动调整技能画像的权重与分类；
c) 宜支持外部数据接入，通过API接口或文件导入方式引入第三方评价信息（如培训记录、认证证书）；
d) 宜设置数据质量校验规则，对异常值或缺失数据进行标记并提示补充。

4.8.2 技能分析与可视化展示功能要求

a) 应采用机器学习算法对数据进行聚类分析，识别参赛者的技能分布特征及潜在能力方向；
b) 应支持自定义分析维度，允许用户按项目类型、时间周期或技能模块筛选特定数据；
c) 宜提供多维可视化工具（如雷达图、热力图、趋势图），直观呈现技能水平、成长轨迹及对比结果；
d) 宜配置智能推荐功能，基于技能画像为参赛者匹配适合的训练资源或赛事机会。

4.8.3 隐私保护与合规性管理功能要求

a) 应遵循最小化原则采集与使用数据，仅收集与技能评估直接相关的必要信息；
b) 应建立数据访问审批流程，确保技能画像的生成与调用符合隐私政策及法律法规要求；
c) 宜采用数据匿名化处理技术，对个人身份信息进行脱敏后用于模型训练与分析；
d) 宜提供用户数据控制权，允许参赛者查看、修改或删除与自身相关的技能画像信息。

5 安全性要求

5.1 物理安全要求

a) 网络和数据安全赛事平台的物理环境，包括但不限于数据中心、服务器机房、网络设施等，应部署于中华人民共和国境内（以下简称“中国境内”）；

b） 物理环境的部署应符合国家相关政策要求，包括国家关于信息基础设施布局、国家安全、信息安全等级保护等政策。

5.2 网络安全要求

a） 网络应采用分层设计，实现数据流量的控制和隔离；
b） 网络设备应定期进行安全更新；
c） 网络设备应配置安全策略，如访问控制列表、端口安全等；
d） 应部署防火墙，对进出网络的数据进行过滤和控制；
e） 应部署入侵检测系统，实时监控网络流量，识别和阻止恶意行为；
f） 应实施网络隔离，如设置DMZ区域，保护核心网络资源；
g） 应采用安全的身份鉴别策略，包括但不限于限制密码长度和复杂度策略、密码更新周期、登录失败处理策略、超时会话等；
h） 应实现网络资源的权限控制，确保只有授权用户能够访问；
i） 应定期检查和更新网络访问控制策略；
j） 应具备安全审计能力，对重要行为和安全事件进行日志记录，应满足国家相关法律法规和行业标准的要求，如《网络安全法》等；
k） 应及时更新安全补丁。

5.3 主机安全要求

a） 操作系统应采用安全的身份鉴别策略，包括但不限于限制密码长度和复杂度策略、密码更新周期、登录失败处理策略、超时会话等；
b） 操作系统应关闭不必要的服务和端口，减少潜在的攻击面；
c） 操作系统应实现用户权限最小化原则，确保用户仅拥有完成其任务所必需的权限；
d） 操作系统应安装防恶意代码工具；
e） 操作系统应及时更新安全补丁；
f） 应具备安全审计能力，对重要行为和安全事件进行日志记录，应满足国家相关法律法规和行业标准的要求，如《网络安全法》等。

5.4 数据库系统安全要求

a） 应采用安全的身份鉴别策略，如限制密码长度和复杂度策略、密码更新周期、登录失败处理策略、超时会话等；
b） 数据库系统应实施访问控制，确保只有授权用户才能访问敏感数据；
c） 数据库系统应定期进行备份，并确保备份数据的安全性；
d） 应具备安全审计能力，对重要行为和安全事件进行日志记录，应满足国家相关法律法规和行业标准的要求，如《网络安全法》等；
e） 应及时更新安全补丁。

5.5 中间件安全要求

a） 应采用安全的身份鉴别策略，包括但不限于限制密码长度和复杂度策略、密码更新周期、登录失败处理策略、超时会话等；
b） 中间件应配置安全参数，如超时时间、错误处理机制等；

c） 中间件应实现传输加密，确保数据在传输过程中的安全性；

d） 中间件应进行安全加固，如关闭不必要的服务和端口；

e） 中间件应及时更新安全补丁；

f） 应具备安全审计能力，对重要行为和安全事件进行日志记录，应满足国家相关法律法规和行业标准的要求，如《网络安全法》等。

5.6 应用安全要求

a） 应遵循安全编码规范，避免常见的安全漏洞，如SQL注入、跨站脚本攻击等；

b） 应定期进行代码审查，及时发现和修复安全漏洞；

c） 应对第三方组件和库进行安全评估，确保其安全性；

d） 应定期进行安全测试，包括但不限于漏洞扫描、渗透测试等；

e） 应对测试发现的安全问题进行及时修复；

f） 应建立安全测试流程，确保新功能上线前的安全性；

g） 应遵循最佳实践，对应用进行安全配置；

h） 应采用安全的身份鉴别策略，包括但不限于限制密码长度和复杂度策略、密码更新周期、登录失败处理策略、超时会话等；

i） 应实现用户数据隔离。应支持用户数据隔离机制，保证不同用户的提交成果及身份信息的隔离安全；

j） 应实现访问控制功能。对不同的角色进行安全标记，从资源抽象、服务及应用等各层面按安全标记和访问控制规则，对角色的操作进行控制；

k） 应实现资源监控。在资源抽象层和服务层，对物理资源应确保主机安全具有资源监控能力，包括不限于对运行状态、CPU、硬盘、内存、网络、虚拟存储和虚拟网络等资源的使用情况进行监控；

l） 应具备安全审计能力，对重要行为和安全事件进行日志记录，应满足国家相关法律法规和行业标准的要求，如《网络安全法》等。

5.7 数据安全要求

a） 重要数据和敏感数据应采用加密算法进行存储，加密算法应符合国家相关标准；

b） 数据存储介质应采取物理安全措施，如放置在安全区域、限制物理访问等；

c） 数据备份应定期进行，并确保备份数据的完整性和可用性；

d） 应确保数据传输通道的安全，防止数据在传输过程中被截获或篡改；

e） 应记录重要数据访问行为，并进行安全审计；

f） 应对敏感数据进行脱敏处理，以保护用户隐私。

6 可靠性与稳定性要求

6.1 可靠性要求

6.1.1 兼容性要求

a） 应支持兼容不同的操作系统、浏览器、设备类型。

其中，

通用操作系统：一般指Linux、Windows、macOS及其他移动端操作系统。平台应能同时支持其中3种及以上；

信创操作系统：指经安全可靠测评的国产操作系统，包括但不限于麒麟系列、统信 UOS 系列、中科方德等。平台应能同时支持2种及以上系列，且在信创操作系统中需实现与通用系统一致的核心功能，且安装、运行、卸载流程无异常。

通用浏览器：如主流浏览器 Chrome、Firefox、Safari、Edge 等。平台应能支持其中3种及以上主流浏览器的当前版本及前一个主要版本，以适应部分用户未及时更新浏览器的情况；

信创浏览器：指国产主流信创浏览器。确保至少能在1款国产浏览器上正常运行，如网页显示正常、交互无故障，支持竞赛答题、文件上传等核心场景。

设备类型：包括桌面设备、移动设备、其他设备。平台应能至少同时支持桌面设备与移动设备；

b） 应支持在中等及以上质量网络环境（丢包率小于等于5%的网络环境）情况下，平台能够持续运行，提供连续服务。

6.1.2 可扩展性要求

a） 平台应具备良好的可扩展性，能够进行功能扩展、性能提升和容量扩充；

b） 平台应支持垂直扩展、水平扩展等多种扩展方式。

6.1.3 数据准确性要求

a） 应支持选手信息、比赛成绩、排名等数据准确录入与计算；

b） 应满足数据采集统计无误差、计算展示正确；

c） 应具备备份数据恢复校验能力。

6.1.4 功能完整性要求

a） 平台应涵盖赛事全流程的各项功能（至少应满足“4 功能要求”章节所述内容），且每个功能都能稳定正常运行；

b） 平台应能按照预期处理各种任务，满足不同类型赛事及赛事各阶段的多样化需求；

其中，

赛事类型：主要包括网络安全、数据安全等赛事类型；

赛事阶段：主要包括注册报名、竞赛、结果查询等。

6.2 稳定性要求

6.2.1 性能优化要求

a） 平台应支持通过对软件算法、数据库查询、缓存机制等方面的优化，不断提升平台性能，以应对不断增长的数据量和复杂的业务逻辑，保证平台在长时间运行过程中始终保持稳定高效的状态。

6.2.2 操作稳定性要求

a） 平台应能在用户的各种常规操作和特殊操作情况下，稳定响应，不会出现错误或异常；

b） 平台应能对用户输入进行严格的校验和过滤，防止非法或不规范的数据对系统造成冲击。

6.2.3 故障恢复能力要求

a） 平台应具备完善的故障检测、预警机制；
b） 平台应具备数据热备份及自动恢复机制。

6.2.4 系统资源合理利用要求

a） 平台应能在不同负载情况下，合理分配和利用系统资源，包括 CPU、内存、网络带宽等；
b） 平台应能确保各功能模块的响应时间保持在合理范围内，不会出现过长延迟或大幅波动。

参 考 文 献

[1]中华人民共和国网络安全法（2016 年 11 月 7 日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[2]中华人民共和国数据安全法（2021 年 6 月 10 日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[3]工业和信息化部等十六部门关于促进数据安全产业发展的指导意见（2023 年 1 月 3 日发布，工信部联网安〔2022〕182号）

[4]GB/T 25069-2022 信息安全技术 术语

[5]GB/T 41479-2022 信息安全技术 网络数据处理安全要求