

2025年柳州市职工职业技能大赛
网络与信息安全管理赛项
技术文件

柳州市职工职业技能大赛组委会

2025 年 9 月

目录

1. 大赛概况	1
1.1. 大赛背景	1
1.2. 大赛目的	1
1.3. 竞赛原则	2
2. 竞赛形式	2
2.1. CTF 赛制	2
3. 试题和评分标准	3
3.1. 内部联赛竞赛平台	3
3.1.1. 实操考核	3
3.1.2. 实操考核答题流程	4
3.2. 评分标准	5
4. 竞赛场地、设施设备安排	5
4.1. 竞赛平台	5
4.1.1. 竞赛平台部署逻辑图	6
4.1.2. 竞赛场地	6
4.1.3. 软硬件支持	7
5. 竞赛规则	8
6. 安全、健康要求	8
6.1. 网络安全要求	8
6.2. 隔离比赛环境	8
6.2.1. 题目与系统安全	8
6.2.2. 参赛者行为规范	8
6.2.3. 数据保护	9
6.3. 物理安全要求	9
6.3.1. 设备管理	9
6.3.2. 场地安全	9
6.4. 健康与纪律要求	9
6.4.1. 时间安排	9
6.4.2. 内容合规	9
6.4.3. 应急预案	9
6.5. 组织建议	9
7. 申诉与仲裁	10
7.1. 申诉条件	10
7.1.1. 允许申诉的情形	10
7.1.2. 不予受理的情形	10
7.2. 申诉流程	10
7.2.1. 提交申诉	10

7.2.2. 初步审核	11
7.2.3. 仲裁阶段	11
7.3. 仲裁规则	11
7.3.1. 仲裁委员会组成	11
7.3.2. 裁决原则	11
7.3.3. 终局性	11
7.4. 补充说明	11
附录 1：考试大纲	13
（一）技术	13
1. 操作系统安全检测与防护	13
2. 数据库安全检测与防护	13
3. 网络攻击与防护	13
4. WEB 应用安全	13
5. 渗透测试技术	14
6. 应急响应与数据恢复	14
7. 移动安全	14
8. LINUX 漏洞挖掘利用与防护（PWN）	14
9. 软件逆向技术	14
10. 杂项	14
11. 工控安全	15
附录 2：竞赛说明	16
1. 竞赛须知	16
2. 竞赛纪律	16

1. 大赛概况

1.1. 大赛背景

当今社会，网络信息化发展迅速，网络与信息安全至关重要。本次大赛紧跟时代步伐，围绕 2025 年广西职工职业技能大赛竞赛项目，结合柳州实际，精心设置了包括网络信息化及新兴技术类在内的竞赛项目，网络与信息安全管理比赛属于网络信息化及新兴技术类，契合了时代发展和产业需求。

大赛以“技能强柳、匠心铸梦”为主题，为广大职工搭建了一个展示风采、切磋技艺的优质平台。通过举办网络与信息安全管理比赛，能够让从事该职业的职工在实战中锤炼专业能力，提升技能水平，同时也促进了该领域人才之间的交流与学习。

1.2. 大赛目的

培养技能人才，推动产业发展：在新时代高质量发展背景下，技能人才是推动产业升级和创新发展的关键。大赛以“技能强柳、匠心铸梦”为主题，旨在加快建设知识型、技能型、创新型产业工人大军，为柳州市网络与信息安全领域培养专业技能人才，助力产业振兴。

提升技能水平，促进交流学习：大赛为广大网络与信息安全管理提供了展示风采、切磋技艺的平台，参赛者可以在实战中锤炼专业能力，提升技能水平，同时也能与其他参赛者交流经验，相互学习，共同进步。

提高社会认知，加强人才梯队建设：通过举办大赛，能够提高网络与信息安全技术的社会认知度，吸引更多人关注和重视该领域，有效推动网络与信息安全技术的人才梯队建设和发展，为新时代中国特色社会主义发展保驾护航。

贯彻政策精神，落实技能竞赛工作：大赛是对相关政策精神的贯彻落实，通过广泛深入开展职业技能竞赛，充分发挥技能竞赛对技能人才培养的引领带动作用，扎实推动以赛促学、以赛促训、以赛促评、以赛促建，促进高质量充分就业，为全区经济社会高质量发展提供技能人才支撑。

1.3. 竞赛原则

合理性原则：大赛工作非简单的技术可以实现，还需要结合参赛对象的能力分布情况，酌情考虑知识点难易、知识面、选手知识掌握等情况，与日常业务紧密结合。

公平性原则：赛事实施应依据国内或国际的相关标准进行，对参赛对象要体现公平性。

规范性原则：赛事执行过程中每一个环节都要严格按照行业规范执行，并保留过程文档，便于事后审计和追溯。

可控性原则：技术实现方法和过程要在双方认可的范围之内，大赛筹备的进度要按照进度的安排，确保主办方对赛事工作的可控性。

整体性原则：考试内容设置应当整体全面，包括网络安全涉及的各个层面，避免由于设计的不合理，形成考题漏洞或者争议。

保密原则：对过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害买卖双方的行为。组织方有权要求技术支撑方在服务结束之后销毁所有和本项目有关的数据和文档。

2. 竞赛形式

2.1. CTF 赛制

线上竞赛模式，采用理论+CTF 实操考核模式，设计 100 道理论题和 10 道 CTF 考题，考生可以根据考题知识点，自由选择题目作答。不限次数地提交答案，答对累积积分，答错不扣分。竞赛排名按积分进行排序，积分相同的，则按时间进行排序，先得分的排名在前。

考核时间为理论 60 分钟，实操 180 分钟，理论题 100 分，CTF 实操题 1000 分，最终成绩按照官方要求比例进行转化核算。考核知识点主要包括操作系统安全、中间件安全、暴力破解、SQL 注入、文件上传、文件包含、XSS、业务逻辑漏洞等。

3. 试题和评分标准

3.1. 内部联赛竞赛平台



3.1.1. 实操考核

实操考核，考生可以不限次数地提交答案，答对累积积分，答错不扣分。竞赛排名按积分进行排序，积分相同的，则按时间进行排序。

CTF 实操考题示意图如下：

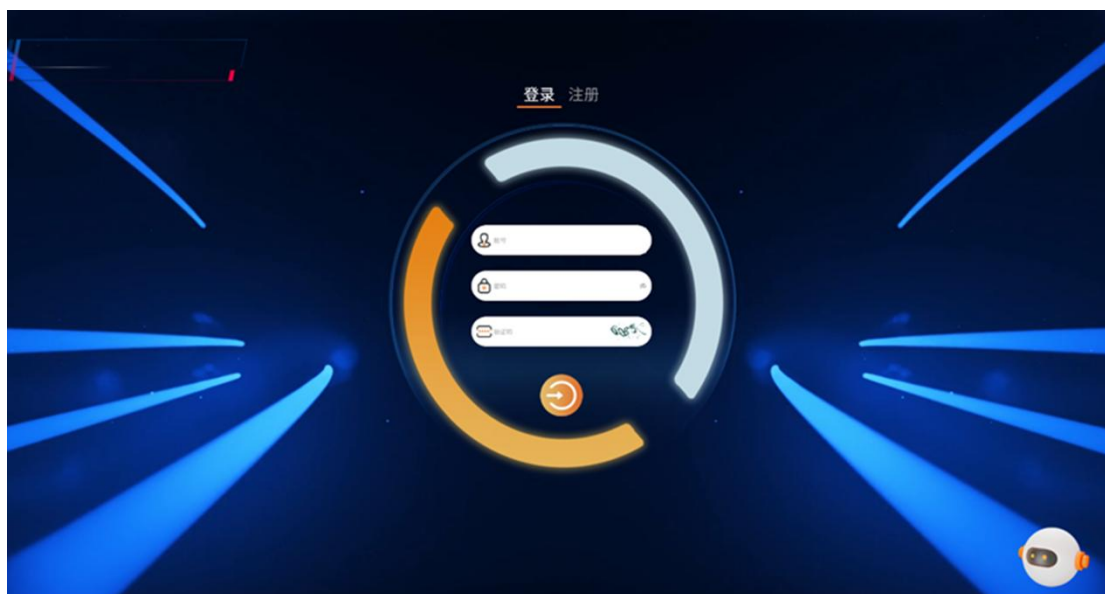
题目				
信息泄露	弱口令	注入	跨站	文件上传
峰回路转 初级	初露锋芒 初级	小试牛刀 初级	初窥门径 初级	扑朔迷离 初级
柳暗花明 中级	---- 中级	庖丁解牛 中级	登堂入室 中级	拨开云雾 中级
文件包含	密码学	越权	任意文件查看和下...	命令执行
夹缝求生 初级	另辟蹊径 初级	鸠占鹊巢 初级	惊鸿一瞥 初级	---- 初级
瞒天过海 中级	剑走偏锋 中级	李代桃僵 中级	鸿鹄之志 中级	---- 中级

CTF 模式知识点覆盖全面、合理，难易交叉，全方位考核参赛选手的信息安

全技能水平。参赛选手可根据自身能力，自主选择考题进行解答。

3.1.2. 实操考核答题流程

①登录竞赛平台



②选择“CTF”模块



③题目作答

根据页面提示，点击访问环境 IP 地址。考生依据自身情况，可以自由选择题目作答。考生解出每道题的 Key 值后，需要将 Key 值输入“答案输入框”，点击“提交”按钮校验。系统会提示 Key 值是否正确。

3.2. 评分标准

CTF 总计 10 小题。每题分数按照题目难易度给分，总分为 1000 分。

每一题均有一血二血三血奖励得分，例如第一小题满分为 80 分，那么第一位做出来的选手得分 80 分，第二位选手得分 75 分，第三位选手得分 70 分，后续所有选手得分为 65 分。竞赛排名按积分进行排序，积分高的排名在前，积分相同的，则按时间进行排序，先得分的排名在前。

实操得分评定方式如下：

- 第一名的实操得分定为满分（核算分数 100 分）。
- 其他名次的实操得分按以下公式计算：

第 X 名实操得分=（第 X 名原始得分÷第一名原始得分）×100

4. 竞赛场地、设施设备安装

4.1. 竞赛平台

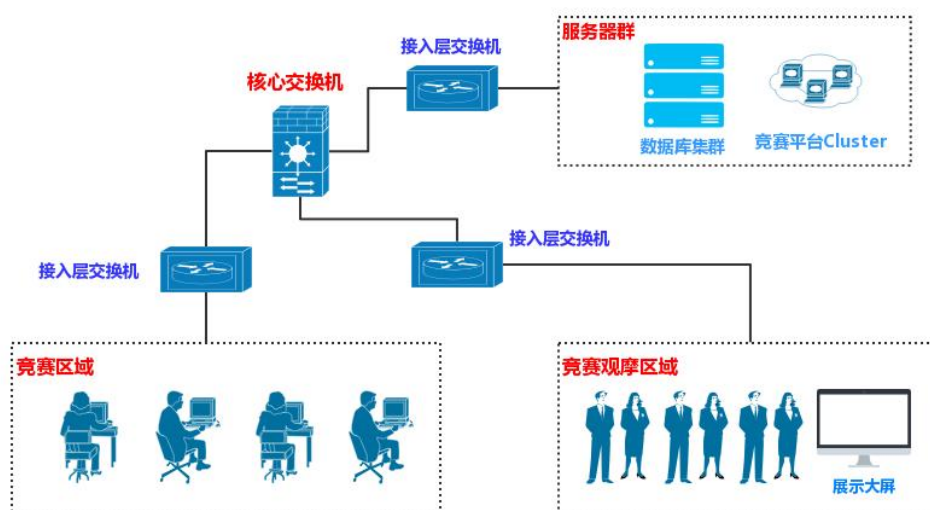
网络与信息安全攻防对抗平台。包括竞赛管理、答题管理、考题环境管理、得分管理、用户管理、展示推送等。

主要参数规格：

项目	规格 / 参数
软件架构	采用 B/S 设计架构，系统具备抗 DDOS 能力，用户可以通过浏览器远程方便地对产品进行访问和管理。
硬件性能指标	1、服务器组件基于 Intelx86 架构 C612 芯片组，2U 机架式结构。 2、CPU：2XEON4310 3、内存：128GDDR4ECC 4、存储：3480GSSD+34THDD（支持 RAID5），8 通道高性能 SASRAID 卡 5、双通道冗余电源， 6、网卡：3 个 100/1000BaseT，2USB 接口。
并发访问数量	并发访问数≥1000，不限 IP 地址授权，不限用户数。

项目	规格 / 参数
单点同时开启虚拟环境数量	虚拟机数量 ≥ 80 。
模式支持	支持闯关、混合、对抗等多种模式，并支持个人和团队分组类型。
	平台和考题相分离，可迅速进行不同类型考题或不同模式的切换，支持定制化技术考题导入，支持 CTF 解题、实战考题等不同类型。
系统判定	系统自动同步生成可视化赛事结果，支持 EXCLE 等导出格式。结果数据支持实时展现总成绩排名、单项知识点排名、答题正确率等。
管理方式	可以在任何 IP 可达地点，提供基于 CONSOL 和 Web 的远程管理，以简单、直观的方式完成策略配置、集中管理等各种任务。
监控方式	支持硬件性能监控包括 CUP、内存、硬盘等；支持系统性能监控包括流量、在线用户等。
平台自身强壮性	平台系统经过严格代码优化和加固，对用户输入信息和权限进行完善的过滤，服务程序功能精简，对考试平台进行严格的策略控制。

4.1.1. 竞赛平台部署逻辑图



4.1.2. 竞赛场地

网络机房。

4.1.3. 软硬件支持

比赛场地提供以下软硬件设备。

建议选手自带笔记本电脑或移动硬盘，提前准备相关知识库与工具。

(1) 竞赛平台+服务器部分

序号	名称	详细描述	数量
1	Haproxy	负载均衡服务器，分解请求，保障系统稳定	2 套
2	MySQL	数据库服务器	2 套
3	XenServer	虚拟操作系统	2 套
4	Redis	用作系统缓存	2 套
5	LAMP	竞赛平台运行环境	2 套

(2) 选手操作机部分

序号	材料名称	数量	版本信息
1	物理机	1 台	微软 Windows 10 以上(64 位)
2	Windows 虚拟机	1 台	已安装网络安全 CTF 比赛常用的编程环境和工具
3	VMware workstation	1 项	VMware workstation 12 pro 及以上版本
4	浏览器	1 项	Chrome / Edge 最新版本

(2) 选手操作机部分

序号	材料名称	数量	版本信息
1	物理机	1 台	微软 Windows 10 以上(64 位)
2	Windows 虚拟机	1 台	已安装网络与数据安全 CTF 比赛常用的编程环境和工具
3	VMware workstation	1 项	VMware workstation 12 pro 及以上版本
4	浏览器	1 项	Chrome / Edge （正式版本）（64 位）

5. 竞赛规则

竞赛具体规则如下：

个人赛：线上理论+CTF 实操

考生可以自主选择理论+CTF 实操答题。

理论+CTF 实操考核，考生可以根据考题知识点，自由选择题目作答。不限次数地提交答案，答对累积积分，答错不扣分。竞赛排名按积分进行排序，积分相同的，则按时间进行排序。其中包含的知识点：密码学、移动应用安全、逆向技术、WEB 漏洞利用、操作系统漏洞利用、应急响应技术、社会工程学等。

6. 安全、健康要求

6.1. 网络安全要求

6.2. 隔离比赛环境

使用独立的局域网或虚拟专用网络（VPN），避免影响学校正常网络。

禁止参赛者访问外部互联网（除非题目需要），防止外部攻击或数据泄露。

6.2.1. 题目与系统安全

所有题目需经过安全测试，避免包含真实漏洞（如 SQL 注入、RCE）影响比赛服务器。

使用容器化技术（如 Docker）隔离每道题目的运行环境，防止横向渗透。

6.2.2. 参赛者行为规范

明确禁止对非比赛目标的攻击（如其他队伍设备、学校公共系统）。

禁止 DoS/DDoS、ARP 欺骗等破坏性攻击，违者取消资格。

6.2.3. 数据保护

不收集参赛者敏感信息（如身份证号），如需注册仅需学号/昵称。

日志记录所有操作，便于追溯违规行为。

6.3. 物理安全要求

6.3.1. 设备管理

提供统一的比赛设备（如机房电脑），或要求参赛者使用指定虚拟机镜像。

6.3.2. 场地安全

确保比赛场地有应急电源和网络备份方案。

安排工作人员巡查，防止作弊或设备损坏。

6.4. 健康与纪律要求

6.4.1. 时间安排

避免长时间连续比赛（建议单场比赛不超过 4 小时），中间安排休息时间。

提供饮水、通风良好的环境，避免过度疲劳。

6.4.2. 内容合规

题目内容需符合法律法规和学校规定，禁止涉及暴力、违法技术（如破解商业软件）。

强调道德黑客精神，仅限技术学习用途。

6.4.3. 应急预案

准备技术支援团队，及时处理突发网络故障或作弊行为。

6.5. 组织建议

赛前培训：开展简短的安全意识培训，说明规则和违规后果。

免责声明：要求参赛者签署协议，明确责任边界。

赛后复盘：清理比赛环境，归档日志，总结安全问题。

7. 申诉与仲裁

7.1. 申诉条件

7.1.1. 允许申诉的情形

题目争议：题目存在歧义、错误或非预期解（如因出题漏洞导致多解）。

技术故障：比赛平台崩溃、网络中断等影响参赛者发挥。

判分错误：Flag 提交正确但系统未正确计分。

违规举报：发现其他队伍作弊（如共享答案、攻击非目标系统）。

7.1.2. 不予受理的情形

因个人操作失误（如误删文件、错误提交 Flag）。

对题目难度或评分规则的主观不满。

7.2. 申诉流程

7.2.1. 提交申诉

时限：比赛结束后的 1 小时内（具体时间可根据赛制调整）。

形式：书面提交（如在线表单或邮件），需包含：

选手姓名、题目编号、具体问题描述。

证据（如截图、日志、解题思路文档）。

实名制：匿名申诉无效。

7.2.2. 初步审核

由赛事组委会或中立裁判组在 30 分钟内确认申诉有效性。

无效申诉直接驳回并说明理由。

7.2.3. 仲裁阶段

技术争议：由出题人或技术专家复核题目设计及提交内容。

违规行为：调取服务器日志、监控录像等证据。

结果公示：通过公告或邮件向全体参赛者公开仲裁结果及依据。

7.3. 仲裁规则

7.3.1. 仲裁委员会组成

至少包含：1 名赛事主办方代表、1 名出题人、1 名第三方教师或校外专家。

利益相关者（如涉及本人所在队伍）需回避。

7.3.2. 裁决原则

技术优先：以日志、代码等客观证据为准。

最小影响：若题目存在漏洞，优先修正评分而非取消题目（如接受非预期解）。

违规处罚：

轻度违规（如误触非目标）：警告并扣分。

严重作弊（如伪造 Flag、破坏系统）：取消比赛资格并通报。

7.3.3. 终局性

仲裁结果为最终决定，一般不再二次申诉（除非提供全新证据）。

7.4. 补充说明

透明性：所有申诉案例及裁决结果应匿名化后公开，作为后续比赛改进参考。

紧急处理：比赛中发现重大漏洞或故障时，裁判有权暂停比赛并统一调整规则。

免责条款：因不可抗力（如断电、自然灾害）导致的比赛中断，主办方可协商延期或部分退款（如有报名费）。

附录 1：考试大纲

（一）技术

1.操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix 等）的常规安全防护技术。能熟练利用系统日志、应用程序日志等溯源攻击途径；掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法。

2.数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB）的库表管理、权限控制等基础技术。熟悉数据库入侵防御、访问控制、身份认证、数据加密等安全措施；深入了解数据库的客户端程序管理、应用系统访问、客户端访问控制、重要操作审计以及数据异地备份等技术实现。

3.网络攻击与防护

熟悉有线和无线网络的攻击和防护技术原理和方法。能运用相关工具及技术手段发现并阻断网络层攻击（例如，中间人攻击、DHCP 攻击、DDOS 攻击、无线 DDOS 攻击、无线 WAPjack 攻击等）、验证各种安全防护手段（如，无线网络 WEP、WPA 和 WPA2 的密码强度）的有效性和强度。

熟悉常见网络设备和安全设备的功能及使用方法。包括：路由器、交换机、防火墙（含 Web 应用防火墙）、入侵检测系统、抗拒绝服务攻击系统、网页防篡改系统、漏洞扫描系统等。

4.Web 应用安全

了解常见 Web 环境（ASPX、PHP、JSP）的搭建方法以及安全配置方法。熟悉中间件和 Web 应用的安全检测与防护方法。能够使用工具或技术手段发现各种 Web 漏洞，例如框架漏洞、权限绕过、弱口令、注入、跨站、文件包含、

文件上传、命令执行、任意文件读取和下载等。

5.渗透测试技术

掌握常规的渗透测试技术。熟练使用各种常见渗透测试工具，渗透测试技术包括：踩点扫描探测、信息收集、暴力破解、常规漏洞利用、Web 权限获取、提权、溢出攻击、植入后门、内网渗透等。

6.应急响应与数据恢复

掌握应急响应和数据恢复的流程和相关技术。包括：入侵取证分析、反取证技术、日志审计分析、日志删除恢复、文件删除恢复、硬盘格式化数据恢复等。

7.移动安全

了解常见移动设备的危害，针对这些有对应防护方法。熟悉应用包的基本结构，掌握移动逆向基本工具的使用，掌握 Java 层和 Native 层的静态和动态调试方法。了解移动应用的基本防护和渗透知识。

8.linux 漏洞挖掘利用与防护（pwn）

掌握 linux 系统下二进制程序漏洞挖掘与利用相关技术，包括 shellcode 编写与利用；缓冲区溢出、格式化字符串攻击、整数溢出、数组越界等漏洞原理、发现、利用和防护方法。

9.软件逆向技术

熟悉计算机的运算流程，掌握软件的运行机制。从处理器底层了解软件的本质。核心是掌握一整套完整的软件逆向技术。包括：汇编语言，软件逆向，混淆。加壳，反调试等一系列对抗手段。

10.杂项

掌握各种古典密码，包括凯撒密码、维吉尼亚密码、仿射密码、摩斯电码等。掌握常见编码算法，包括：base64、URL 等。熟悉信息隐写的原理，掌握针对各

种类型载体的隐写以及分析提取的方法，熟练使用常见隐写分析工具，包括 binwalk、01Editor、stegsolve 等。了解各种协议的原理，包括 TCP、UDP、HTTP、FTP 等，掌握数据包分析工具的使用。

11.工控安全

工控协议流量分析，工控取证分析，工控涉及的密码学分析破解。

附录 2：竞赛说明

1.竞赛须知

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 Key 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 Key 将无法提交验证。

3.CTFflag 出现的形式为：flag{xxxxxxxx}，提交 flag 时，只需要提交“xxxxxxxx”，不要携带 flag{}。CTFflag 可以无限提交，回答正确加分，回答错误不扣分。CTF 没有题号的顺序，可以任意选择作答，所有的 flag 都在同一个答案输入框中提交。

4.严禁利用扫描器对竞赛平台进行恶意扫描、暴力猜解 Key 值、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，或者其他与竞赛相关的事宜，请举手示意，切勿大声呼喊。

2.竞赛纪律

(1) 参赛选手凭本人身份证原件进入赛场；

(2) 参赛选手在竞赛开始前 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）竞赛过程中或竞赛后如有任何问题（包括反映竞赛或其他问题），应立即举手示意，等待现场工作人员帮助；

（8）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；

（9）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；

（10）比赛过程中禁止使用 CC/DDOS/ARP/中间人攻击等恶意攻击工具影响比赛公平正常进行，一经发现，所属队伍离场，本轮分数记 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队伍解题方法/得分思路，如果发现回答有误，疑似通过作弊获得分数将对队伍扣分，严重者取消队伍参赛资格；

（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。