第十六届山东省职业院校技能大赛

中职组“网络安全”赛项规程

一、赛项名称

赛项名称：网络安全

英文名称：[Cyber Security](http://www.baidu.com/link?url=Ltb-4t1FNAs7ZPE6xtBnVYCgbAb-538XHRCKjaCuJRg5urKbS0R2HQWwtRjzqW6_5TWgxixiDaVIqbwDE2E0OHejjwXEgTCBXWAi_qxQguuYy2FVw5RNy3Pcanpmcg-_)

赛项组别：中职组

专业大类：电子与信息大类

二、竞赛目的

网络空间已经成为陆、海、空、天之后的第五大主权领域空间，习总书记强调：没有网络安全就没有国家安全。为引领全国中职学校紧跟网络安全技术和产业的发展，为国家和社会培养急需的网络安全技能型人才，国家教育部联合多部委特举办本赛项，将网络安全行业新业态、新技术、新标准等纳入比赛内容，以赛促教，以赛促学，以赛促改，发挥示范引领作用，推进“岗课赛证”综合育人。

三、竞赛内容

**（一）竞赛内容**

主要考核参赛选手网络系统安全策略部署、信息保护、网络安全运维管理、网络安全事件应急响应、网络安全数据取证、应用安全、代码审计等综合实践能力，具体包括：

|  |  |  |
| --- | --- | --- |
| **竞赛阶段** | **竞赛任务** | **竞赛内容** |
| A模块 | 基础设施设置与安全加固 | 登录安全加固、数据库加固（Data）、Web 安全加固(Web)、流量完整性保护（Web,Data）、事件监控、服务加固、防火墙策略等； |
| B模块 | 网络安全事件响应、数字取证调查和应用安全 | 网络安全事件、数字取证调查和应用安全” 内容主要包括：数据分析、数字取证、内存取证、漏洞扫描与利用、操作系统渗透测试、应急响应等； |
| C模块 | CTF 夺旗-攻击 | 假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，了解网络黑客的心态，从而改善您的防御策略； |
| D模块 | CTF 夺旗-防御 | 假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器,参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。 |

**（二）竞赛分值权重和时间安排**

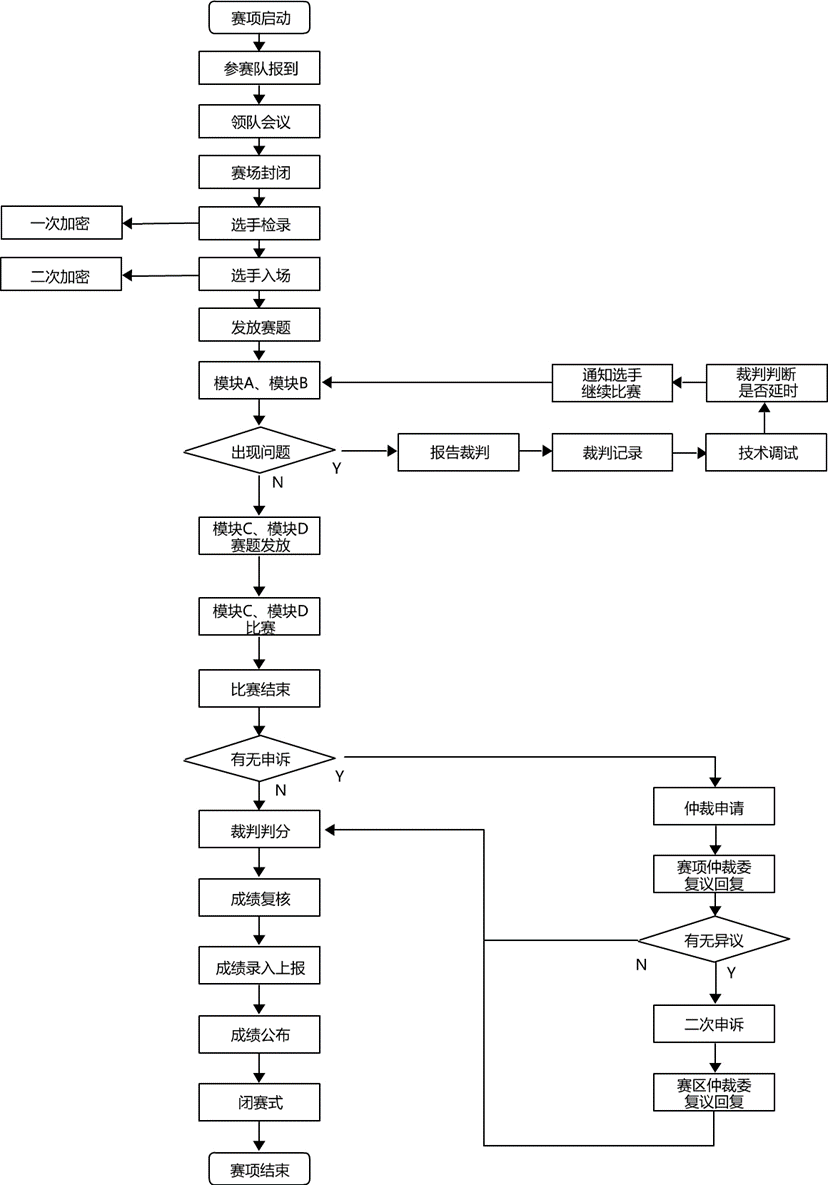
|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **模块名称** | **竞赛时间（小时）** | **权值** |
| A | 基础设施设置与安全加固 | 3 | 20% |
| B | 网络安全事件响应、数字取证调查和应用安全 | 40% |
| C | CTF 夺旗-攻击 | 3 | 20% |
| D | CTF 夺旗-防御 | 20% |
| 总计 | | 6 | 100% |

四、竞赛方式

本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。每个参赛队由2名选手组成，同一学校报名参赛队不超过1支。指导教师须为本校专兼职教师，每个参赛队限报2名指导教师。

五、竞赛流程

**（一）竞赛流程图**

****

**（二）竞赛场次**

竞赛限定在1天内进行，竞赛场次为2场，每场3小时，总竞赛时间为6小时。

|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **模块名称** | **竞赛时间（小时）** | **权值** |
| A | 基础设施设置与安全加固 | 3 | 20% |
| B | 网络安全事件响应、数字取证调查和应用安全 | 40% |
| 午餐 | |  |  |
| C | CTF夺旗-攻击 | 3 | 20% |
| D | CTF夺旗-防御 | 20% |
| 总计 | | 6 | 100% |

六、竞赛命题

（一）本赛项建立竞赛试题库，竞赛前1个月发布在“山东省职业院校技能大赛网:“http://sdskills.sdei.edu.cn/”。

（二）赛项样题见附件一。

七、竞赛规则

（一）报名资格

参赛选手须为2023年度在籍全日制中等职业学校学生；五年制全日制高职一至三年级（含三年级）在籍学生可参加竞赛。参赛选手不限性别，年龄须不超过21周岁，年龄计算的截止时间以2023年10月30日为准。往届本赛项山东省职业院校技能大赛获一等奖学生，不再参加本项目比赛。

（二）竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

（三）竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前20分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

（六）竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非参赛选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（七）竞赛结束（或提前完成）后，参赛选手起立，在确认后不得再进行任何操作，按顺序离场。

（八）最终竞赛成绩经复核无误及裁判长、监督长签字确认后，在指定地点，以纸质形式在指定点向全体参赛队进行提前公布，各参赛队无异议后在闭赛式上予以宣布。

（九）本赛项各参赛队最终成绩由承办单位信息员录入赛务管理系统。承办单位信息员对成绩数据审核后，将赛务系统中录入的成绩导出打印，经赛项裁判长审核无误后签字。承办单位信息员将裁判长确认的电子版赛项成绩信息上传赛务管理系统，同时将裁判长签字的纸质打印成绩单报送大赛执委会。

（十）赛项结束后专家工作组根据裁判判分情况，分析参赛选手在竞赛过程中对各个知识点、技术的掌握程度，并将分析报告报备大赛执委会办公室，执委会办公室根据实际情况适时公布。

（十一）赛项每个竞赛环节裁判评分的原始材料和最终成绩等结果性材料经监督组人员和裁判长签字后装袋密封留档，并由赛项承办院校封存，委派专人妥善保管。

八、竞赛环境

（一）竞赛场地。竞赛场地需保证良好的采光、照明和良好通风；提供稳定的水、电和供电应急设备，提供足够的干粉灭火器材。同时提供所有指导教师休息室1间。

（二）竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备竞赛所需的软硬件平台，为参赛队提供标准竞赛设备。

（三）竞赛工位。工位间距和场地空间必须符合竞赛要求，每个竞赛工位上标明编号并用隔离带隔离，确保参赛队之间互不干扰，每个竞赛工位配备2把工作椅（凳）。

（四）服务区提供医疗等服务保障，并用隔离带隔离。

九、技术规范

该赛项结合企业职业岗位对人才培养需求，涉及的信息网络安全工程在设计、组建过程中，主要有以下8项国家职业标准，参赛选手在实施竞赛项目中要求遵循如下规范：

|  |  |  |
| --- | --- | --- |
| **序号** | **标准号** | **中文标准名称** |
| 1 | GA/T 1389-2017 | 《信息安全技术网络安全等级保护定级指南 》 |
| 2 | GB 17859-1999 | 《计算机信息系统安全保护等级划分准则》 |
| 3 | GB/T 20271-2006 | 《信息安全技术信息系统通用安全技术要求》 |
| 4 | GB/T 20270-2006 | 《信息安全技术网络基础安全技术要求》 |
| 5 | GB/T 20272-2006 | 《信息安全技术操作系统安全技术要求》 |
| 6 | GB/T 20273-2006 | 《信息安全技术数据库管理系统安全技术要求》 |
| 7 | GA/T 671-2006 | 《信息安全技术终端计算机系统安全等级技术要求》 |
| 8 | GB/T 20269-2006 | 《信息安全技术信息系统安全管理要求》 |

十、技术平台

**（一）竞赛器材**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **设备要求** |
| 1 | 网络安全竞赛平台 | 1 | 磐云网络空间安全实战平台  1. 能完成基础设施设置、安全加固、安全事件响应、网络安全数据取证、应用安全、CTF夺旗攻击、 CTF夺旗防御等知识、技能内容竞赛环境实现，能有效支持300人规模，具备基于本规程竞赛内容同一场景集中答题环境。  2. 标配2个千兆以太口，Intel处理器，大于等于16G 内存，SSD +SATA硬盘。可扩展多种虚拟化平台，支持集群管理，同步采用增量备份的方式，虚拟化管理采用标准libvirt接口；支持多用户并发在线竞赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板，全程无需手工配置地址，VLAN与IP可根据竞赛要求自行设定；提供单兵闯关、分组混战等实际对战模式，阶段间无需人工切换，系统自动处理；提供超过20种不同级别70个的攻防场景；模块B、C全过程自动评判，支持竞赛过程图像元素上传，排名判定策略大于等于12种；自定义动画态势展示，成绩详细分析；支持监控异常虚拟机，同时检测FTP、HTTP、ICMP、SMTP、SSH、TCP和UDP协议，服务端口支持在有效范围内的服务端口；支持全程加密，支持加密文件导入，加密方式为非对称加密，设备能随机生成密码。 |
| 2 | PC机 | 2 | CPU 主频>=2.8GHZ,>=四核四线程；内存>=8G；硬盘>=500G；支持硬件虚拟化。 |

**（二）软件技术平台：**

竞赛的应用系统环境主要以Windows和Linux系统为主，涉及如下版本：

1．物理机安装操作系统：微软 Windows 7(64位)中文试用版或微软 Windows 10(64位)中文试用版。

2．虚拟机安装操作系统：

Windows系统（试用版）：Windows XP、Windows 7、Windows 10、Windows Server2003及以上版本（根据命题实际确定）。

Linux系统：Ubuntu、Debian、CentOS（具体版本根据命题实际确定）。

3.其他主要应用软件为（实际竞赛环境可能不仅限于以下软件）:

VMware workstation 12 pro 及以上版本免费版

Putty 0.67及以上版本

Chrome 浏览器 62.0及以上版本

RealVNC 客户端 4.6及以上版本

十一、成绩评定

**（一）裁判评分方法**

现场裁判组监督现场机考评分，评分裁判负责参赛选手提交作品评分，裁判长负责竞赛全过程。

竞赛现场派驻监督员、裁判员、技术支持队伍等，分工明确。现场裁判员负责与参赛选手的交流沟通及试卷等材料的收发，负责设备问题确认和现场执裁；技术支持工程师负责所有工位设备应急，负责执行裁判确认后的设备应急处理。

**（二）成绩产生办法**

1.评分阶段：

|  |  |  |  |
| --- | --- | --- | --- |
| **竞赛阶段** | **阶段名称** | **任务阶段** | **评分方式** |
| 模块A  权重40% | 基础设施设置、安全加固 | 任务1…N | 裁判客观评分 |
| 模块B  权重60% | 安全事件响应、网络安全数据取证、应用安全 | 任务1…N | 机考评分 |
| 模块 C  权重 20% | CTF 夺旗攻击 | 系统攻防演练 | 机考评分 |
| 模块 D  权重 20% | CTF 夺旗防御 | 系统攻防演练 | 裁判客观评分 |

2.模块A、模块B评分规则

模块A与模块B总分为600分,分为N个任务，每道题的具体分值在赛题中标明；模块A基础设施设置、安全加固部分评分由评分裁判客观评分；模块B安全事件响应、网络安全数据取证、应用安全等部分由系统自动评分和排名，对外公开显示。

3.模块C、模块D评分规则

模块C总分为200分，按照选手获得攻击“FLAG”的值得到相应的分数。系统自动评分和排名，对外公开显示。

模块D总分为200分，按照选手答题内容，由评分裁判进行客观评分。

选手在答题过程中不得违反竞赛试题要求答题，不得以违规形式获取得分，不得违规攻击裁判服务器、网关、系统服务器等非靶机目标，如检测选手有违规攻击行为，警告一次后若继续攻击，判令该队终止竞赛，清离出场。

3.奖项设置

本赛项设参赛选手团体一、二、三等奖。以赛项实际参赛队(团体赛)总数为基数，一、二、三等奖获奖比例分别为10%、20%、30%(小数点后四舍五入)。

4.成绩复核

为保障成绩评判的准确性，监督仲裁组对赛项总成绩排名前30%的所有参赛队伍的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖率不低于 15%。监督仲裁组需将复检中发现的错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。若复核、抽检错误率超过 5%，裁判组需对所有成绩进行复核。

5.成绩公示

赛项成绩解密后，在赛项执委会指定的地点，以纸质形式向全体参赛队进行公布。

十二、赛场预案

为保障赛项顺利进行，避免竞赛过程中出现可能的不可控的紧急 情况，赛项预案由赛项可靠性设计、故障的应急处理方案两部分组成。

**（一）赛项可靠性设计**

1.电力系统可靠性设计供电负荷匹配电力要求，防止电子设备运行过程中过载导致火灾隐患或电力中断；提供三项电源接地保证，杜绝运行过程中静电可能 导致设备重启、短路、漏电等安全威胁；布线强弱电分离，防止发生干扰；各区域供电保障独立，相互不干扰。

2.弱电系统可靠性设计弱电系统必须保证良好的运行状态，系统应具备长期和稳定的工作能力，遇到突发状况时应存在快速解决方法，保证系统可靠运行。弱电系统应与电力系统隔离部署，防止干扰造成故障。

3.网络设备可靠性设计 网络设备必须要运行稳定，满足带宽要求，预留端口备份，通信 线缆、设备预留备份，具备故障快速恢复机制，提供必要的冗余备份设计。

4.攻防平台可靠性设计平台必须支持集群功能，在大规模流量下支持负载分担，同时可为竞赛数据提供备份、回退机制。具备冗余备份机制，在最短时间内恢复故障问题。平台应提供访问控制机制，具备防攻击手段，保障平台运行稳定。

5.PC 可靠性设计PC的部署必须保证良好的运行状态，遇到突发状况时应存在快速解决方法，保证系统可靠运行。系统规格必须满足要求，保证良好的性能和稳定的运行。

**（二）故障的应急处理方案**

1.参赛选手PC 故障

如参赛选手PC遇到故障，先判断其为硬件故障还是软件故障。 软件故障或出现卡顿现象则对PC进行重启，因PC配备还原卡，可将系统恢复至初始状态，故障恢复时间约30秒；硬件故障经过现场裁判允许后更换备用机，故障恢复时间约1分钟。键盘、鼠标故障及时更换，恢复时间约1-3分钟。不会对学生成绩产生影响。

2.竞赛工位线缆连接故障

竞赛工位如遇到网络连接问题，现场裁判判定线缆物理连接问题，非选手设置操作导致，应及时更换备用线缆，故障恢复时间约30秒；竞赛工位两条以上网线物理故障，经现场裁判允许为其更换竞赛工位，故障恢复时间约 3-5 分钟。

3.竞赛工位电力故障

如遇竞赛工位电力故障，经裁判长允许更换备用工位。故障恢复时间3-5分钟。

4.网络设备交换机故障

更换备用交换机，故障恢复时间约5-10分钟；跳线线缆故障及时更换备用线缆（光纤及网线），故障恢复时间约 3-5 分钟。

5.攻防平台集群故障

服务器集群主设备故障，启用备用集群设备，数据互备份，集群恢复时间约 5-10 分钟。服务器集群从设备故障，更换备用设备，恢复时间约5-10分钟。成绩实时保存，不会对学生成绩产生影响。

6.WEB应用防火墙故障

如遇WAF设备故障，影响访问，取消防护策略或取消WAF设备连接，故障恢复时间约1-3分钟。

7.服务器区供电问题

若服务器区发生供电问题，UPS电源可支持20-30分钟。

十三、申诉与总裁

大赛采取二级仲裁机制。各赛项设赛项仲裁工作组，大赛执委会设仲裁委员会。各参赛队对不符合大赛和赛项规程规定的仪器、设备、工装、材料、物件、计算机软硬件、竞赛使用工具、用品，竞赛执裁、赛场管理，以及工作人员的不规范行为等，可向赛项仲裁工作组提出申诉。申诉主体为参赛队领队。申诉启动时，领队向赛项仲裁工作组递交亲笔签字同意的书面申诉报告。申诉报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。非书面申诉不予受理。

提出申诉的时间应在竞赛结束后（选手赛场竞赛内容全部完成）2小时内，超过时效不予受理。赛项仲裁工作组在接到申诉报告后的2小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由市（高职院校）领队向仲裁委员会提出申诉。仲裁委员会的仲裁结果为最终结果。申诉方可随时提出放弃申诉。

十四、竞赛观摩

本赛项将提供公开观摩区，使用大屏幕实时展示网络安全竞技过程。竞赛环境依据竞赛需求和职业特点设计，在竞赛不被干扰的前提下安全开放部分赛场。观摩人员需佩戴观摩证件在工作人员带领下沿指定路线、在指定区域内到现场观赛。

十五、竞赛直播

本赛项赛前对赛题保密、设备安装调试、软件安装等关键环节进行实况摄录。竞赛过程采用实况转播的形式，对竞赛的开闭幕式、竞赛过程全程摄录。本赛项在赛后将制作大赛制作优秀选手采访、优秀指导教师采访、裁判专家点评和企业人士采访视频资料。

十六、竞赛须知

**（一）参赛队须知**

1.参赛队应该参加赛项承办单位组织的闭赛式等各项赛事活动。

2.在赛事期间，领队及参赛队其他成员不得私自接触裁判，凡发现有弄虚作假者，取消其参赛资格，成绩无效。

3.所有参赛人员须按照赛项规程要求按照完成赛项评价工作。

4.对于有碍竞赛公正和竞赛正常进行的参赛队，视其情节轻重，按照相关管理办法给予警告、取消竞赛成绩、通报批评等处理。

**（二）参赛领队须知**

1.领队应按时参加赛前领队会议，不得无故缺席。

2.领队负责组织本参赛队参加各项赛事活动。

3.领队应积极做好本参赛队的服务工作，协调各参赛队与赛项组织机构、承办院校的对接，按照防疫要求做好团队各项防疫工作。

4.参赛队认为存在不符合竞赛规定的设备、工具、软件，有失公正的评判、奖励，以及工作人员的违规行为等情况时，须由领队向赛项仲裁组提交书面申诉材料。各参赛队领队应带头服从和执行申诉的最终仲裁结果，并要求指导教师、选手服从和执行。

**（三）参赛选手须知**

1.各参赛选手要按照防疫要求做好个人和团队防疫工作，发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2.参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

3.参赛选手应按照规定时间抵达赛场，凭统一印制的参赛证、有效身份证件检录，按要求入场，不得迟到早退。请勿携带任何电子设备及其他资料、用品进入赛场。

4.参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

5.参赛选手应增强角色意识，科学合理做好时间分配。

6.参赛选手应按有关要求在指定位置就坐。

7.参赛选手须在确认竞赛内容和现场设备等无误后开始竞赛。在竞赛过程中，确因计算机软件或硬件故障，致使操作无法继续的，经项目裁判长确认，予以启用备用计算机。

8.各参赛选手必须按规范要求操作竞赛设备。一旦出现较严重的安全事故，经总裁判长批准后将立即取消其参赛资格。

9.参赛选手需详细阅读赛题中竞赛文档命名的要求，不得在提交的竞赛文档中标识出任何关于参赛选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

10.竞赛时间终了，选手应全体起立，结束操作，将资料和工具整齐摆放在操作平台上，经工作人员清点后可离开赛场。离开赛场时不得带走任何资料。

11.在竞赛期间，未经执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

**（五）工作人员须知**

1.树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项组织部门的领导下，按照各自职责分工和要求认真做好岗位工作。

2.所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3.注意文明礼貌，保持良好形象，熟悉赛项指南。

4.自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5.提前30分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

6.熟悉竞赛规程，严格按照工作程序和有关规定办事，遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

7.工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8.保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。