

第47届世界技能大赛宁波市选拔赛
网络安全项目
技术文件

2023年 03月

目录

目录	- 2 -
1.项目简介	4
1.1 项目描述	4
1.2 竞赛目的	4
2.竞赛团队及能力要求	5
2.1 团队选手人数	5
2.2 选手年龄要求	5
2.3 选手应具备的能力	5
3.竞赛项目	10
3.1 竞赛模块	11
3.2 模块简述	11
3.2.1 模块 A	11
3.2.2 模块 C	11
3.3 命题方式	12
3.4 命题方案	13
4.评分标准	13
4.1 测量评分	13
4.2 评分流程说明	14
4.3 统分方法	14
4.4 裁判组构成和分工	14

4.4.1 裁判组.....	14
4.4.2 裁判任职条件.....	14
4.4.3 裁判分工方案.....	15
5.竞赛相关设施设备	15
5.1 每工位设备清单.....	15
5.2 软件技术平台	16
5.3 场地禁止自带使用的设备和材料.....	17
6.项目特别规定	17
7.赛场布局要求	18
8.健康安全	18
9.绿色环保.....	19

1.项目简介

本项目技术说明是对竞赛项目内容的框架性描述，正式比赛内容及要求以竞赛当日公布的为准。

1.1 项目描述

网络安全项目需要选手安装、配置和强化计算机、服务器、防火墙、网络设备和相关软件等内容，以符合网络安全专业人员和信息安全分析师典型任务的要求。项目旨在测评参赛选手在信息系统的安全运维管理、安全评估、渗透测试、应急响应和调查取证中使用的一系列技术技能。参赛选手应同时具备表达、书写、沟通、协调等能力，具有较高综合素质。测试项目将分为 2 个不同的任务，安排在 1 天的竞赛期间依次进行：

- (1) 信息系统环境安全加固
- (2) 夺旗行动（CTF）挑战

1.2 竞赛目的

为全面贯彻落实习近平总书记关于对技能人才工作的重要指示精神和省委省政府决策部署，加强技能人才队伍建设，引领大规模职业培训工作和岗位练兵活动深入广泛开展，弘扬劳模精神和工匠精神，营造劳动光荣的社会风尚和精益求精的敬业风气要求，通过组织世界技能大赛市赛选拔赛，促进技能竞赛和技能人才培养工作科学有序地发展。

参照世界技能大赛的技术要求和规则标准，选拔选手代表宁波市备战第 47 届世赛浙江省赛选拔赛；同时，通过市选拔赛使参赛选手、裁判等相关人员进一

步熟悉世赛技术要求，加深对相关项目技术技能发展趋势的了解与认识。

2.竞赛团队及能力要求

2.1 团队选手人数

网络安全为团队项目，每参赛队由两名选手组成。

2.2 选手年龄要求

参赛选手应为中国大陆地区 1999 年 1 月 1 日以后出生。

2.3 选手应具备的能力

本项目参赛选手应熟练掌握的知识点及应具备的特定技能，参照第 47 届世界技能大赛该项目标准规范编制，可作为竞赛选手训练及准备的参考。

以下能力描述分为几个部分，每部分使用总分的百分比来区分它的重要性。竞赛测试项目及评分方案应尽可能的反映选手参照项目技能要求中所列知识点和技能的熟练度，大赛允许 5% 的偏差。

表 2.3.1 项目技能要求

项目		相关重要性(%)
1	工作组织和管理	5
	个人（选手）需了解和理解： <ul style="list-style-type: none">•健康与安全相关法规、义务、规定和文档•必须使用个人防护用品（PPE）的场合，如：静电防护（ESD、静电放电）•在处理用户设备和信息时的诚信和安全的重要性•废物回收、安全处置的重要性•计划、调度和优先处置的方法•在所有的工作实践过程中,准确、检查和注意细节的重要性•系统性开展工作的重要性	
	个人（选手）应具备的能力： <ul style="list-style-type: none">•遵守健康和标准、规则和规章制度•保持安全的工作环境•识别并使用适当的个人静电防护设备	

	<ul style="list-style-type: none"> •安全、妥善地选择、使用、清洁、维护和储存工具和设备 •规划工作区域，以最大化工作效率，并维持日常整洁的相关规定。 •有效地工作，并定期检查进度和结果 •采取全面有效的研究方法，确保知识不断更新 •主动尝试新方法、新系统和愿意接受变革 	
2	通讯和人际沟通技巧	10
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> •倾听作为有效沟通一部分的重要性 •作为同事的角色、要求和最有效的沟通方式 •与同事和管理人员建立和保持创造性的工作关系的重要性 •有效的团队合作技巧 •消除误会和化解冲突的技巧 •管理紧张和愤怒情绪 	
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> •运用认真倾听和提问的良好技巧，加深对复杂情境的理解 •与同事进行持续有效的口头和书面沟通 •认识到并适应同事不断变化的需求 •积极推动，建立强大而有效的团队 •与同事分享知识和专业知识，形成相互支持的学习文化 •有效管理紧张/愤怒，并给他人可以解决问题的信心 	
3	安全规定条款	15
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> •信息技术风险管理标准、政策、要求和过程。 •网络防御和漏洞评估工具及其功能。 •操作系统 •计算机编程相关概念，包括计算机语言、编程、测试、调试和文件类型。 •应用于软件开发的网络安全和隐私原则和方法。 	
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> •在设计和记录总体程序测试和评估过程时，应将网络安全和隐私原则应用于组织要求（与保密性、完整性、可用性、身份验证、不可否认）相关。 •独立进行综合测试，包括管理、运行和技术安全控制、IT 系统内部或者源自 IT 系统的增强控制功能等，判断/决定整体控制效果 •开发、创建和维护新的计算机应用程序、软件、或专门应用程序 •修改现有的计算机应用程序、软件、或专门应用程序 •分析新的或者现有计算机应用程序、软件和或专业们的应用程序的安全状况，提供可用的结果。 •开发和维护业务、系统和信息流程以支持企业任务需求 •开发描述基线和目标体系结构的信息技术 (IT) 规则和要求 •确保利益相关各方安全需求，保护企业运营和商业流程在企业架构的各个方面得到正常处理,包括参考模型、部分和解决方案架构(segment and solution architectures)、确保系统支持企业的运营和商业流程。 •进行软件和系统工程和软件系统研究并开发新功能，确保网络安全功 	

	<p>能集成于其中。</p> <ul style="list-style-type: none"> •进行综合技术研究，对网络安全系统中可能的薄弱环节进行评估。咨询相关人员，评估功能需求，并将功能需求转换为技术解决方案。 •计划、准备和实施系统测试 •根据技术规范和要求，进行分析、评估并报告结果 •设计、开发、测试和评估信息系统的安全情况，涵盖系统系统开发生命周期。 	
4	操作、维护、监督和管理	15
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> •查询语言，如 SQL (结构化查询语言) 和数据库系统。 •数据备份和恢复、管理和数据标准化策略。 •网络协议，如 TCP/IP、动态主机配置、域名系统 (DNS) 和目录服务。 •防火墙概念和功能 (例如，单点身份验证/审核/策略执行 (或强制策略)、恶意内容的邮件扫描、PCI 和 PII 遵从性数据匿名化、数据丢失保护扫描、加速加密操作、SSL 安全、REST/JSON 处理)。 •网络安全体系结构的概念，包括拓扑、协议、组件和原则 (例如，纵深防御的应用)。 •系统管理、网络和操作系统硬化技术。 •组织信息技术 (IT) 用户安全策略 (例如，帐户创建、密码规则、访问控制)。 •信息技术(IT)安全原则和方法(如防火墙、非军事区 (控制区)、加密)。 •身份验证、授权和访问控制方法。 •网络安全、漏洞和隐私原则。 •进行培训和教育需求评估的选择性原则和过程。 •学习管理系统及其在管理学习中的应用。 •网络竞赛是一种通过在模拟的现实环境中提供亲身体会来开发技能的方法。 •网络法律与法律方面的考虑及其对网络规划的影响 	
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> •开发并管理数据库和/或数据管理系统，确保存储、查询、保护和数据应用。 •管理并实施流程和工具，确保机构可以识别、存档、获取知识资产和信息内容。 •处理问题，安装、配置、排除故障，并按照客户需求或咨询提供维护和培训。 •安装、配置、测试、运行、维护和管理网络和防火墙，包括硬件和软件，确保所有信息传输方面的共享、传输，对信息安全和信息系统给提供支持。 •安装、配置、调试和维护服务器（硬件和软件），确保信息保密性、完整性和可用性。 •管理账户、防火墙和补丁。 •控制访问、密码和账户创建和管理。 •为了设计信息系统解决方案，检查机构的现有计算机系统和流程，帮 	

	<p>助该机构更安全、更快捷和更高效的运营。</p> <ul style="list-style-type: none"> •通过对商业和信息技术（IT）的需求和限制做出回应，使得二者协同工作。 •协助监督信息系统或网络的网络安全项目，管理机构内部的信息安全可能存在的问题、特定的项目，或其他需要负责的各方面，包括策略、人员、基础架构、需求、政策加强、应急计划、安全意识和其他资源。 	
5	保护和防卫	15
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> •文件系统实现（例如，新技术文件系统 [NTFS]、文件分配表 [FAT]、文件扩展名 [EXT]）。 •系统文件（如日志文件、注册表文件、配置文件）包含相关信息以及在何处查找这些系统文件。 •网络安全体系结构的概念，包括拓扑、协议、组件和原则（例如，纵深防御的应用）。 •行业标准和组织性接受的分析原则、方法和工具来识别漏洞。 •威胁调查、报告、调查工具和法律/条例。 •事件类别、响应和处理方法。 •网络防御和漏洞评估工具及其功能。 •对于已知的安全风险的应对措施设计 •身份验证、授权和访问方法（例如基于角色的访问控制、强制访问控制和任意访问控制）。 	
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> •使用防护措施和不同渠道收集的信息，以识别、分析和报告发生的、或可能发生的网络事件，以保护信息、信息系统和网络免于威胁。 •测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理的计算机网络防护服务提供商的网络和资源。 •监视网络，及时修订未授权的活动 •在所属的领域对危机或者紧急状态做出有效响应，在自己的专业领域中降低直接的和潜在的威胁。 •使用缓解措施、准备措施，按照要求做出响应和实施恢复步骤，以最大化存活率，保存财产和信息的安全。 •调查和分析所有的相关响应活动。 •对威胁和漏洞进行评估 •确定与可接受的配置、企业或本地策略的偏差 •评估风险水平，制定和/或建议在业务和非运营情况下采取适当的缓解措施。 	
6	分析	10
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> •网络威胁行为者，他们的资本和他们的方法。 •用于检测各种可利用的活动的方法和技术。 •网络情报/信息收集能力和存储资料库。 •网络威胁和漏洞。 •网络安全基础知识（例如加密、防火墙、认证、诱捕系统、外围保护）。 	

	<ul style="list-style-type: none"> •漏洞信息传播源 (例如, 警报、通知、勘误表和公告)。 •哪些系统文件 (如日志文件、注册表文件、配置文件) 包含相关信息以及在何处查找这些系统文件。 •开发工具的结构、方法和策略 (例如, 嗅探、记录键盘) 和技术 (例如获取后门访问、收集/机密数据、对网络中的其他系统进行漏洞分析)。 •预测和/或模拟威胁能力和行动的内部策略。 •内部和外部合作伙伴的网络操作能力和工具。 •目标开发 (即概念、角色、责任、产品等) •系统开发过程遗留物 (System Artefacts) 和司法鉴定应用案例 	
	<p>个人 (选手) 应具备的能力:</p> <ul style="list-style-type: none"> •识别和评估网络安全罪犯或外国情报机构的能力和活动 •出具调查结果, 以帮助初始化或支持执法和反情报调查或活动。 •分析搜集到的信息, 找到系统弱点和潜在可被利用的环节。 •分析来自情报界的不同渠道、不同学科和不同机构的威胁信息, •根据背景情况, 同步和放置情报信息, 找出可能的含义 (影响)。 •应用来自一个或多个不同地区、国家、非政府机构和/或技术领域的最新知识。 •应用语言、文化、和技术专业知识, 进行信息收集、分析和其他网络安全活动。 •识别、保存和使用系统开发过程遗留物并用于分析 	
7	收集与操作	15
	<p>个人 (选手) 需了解和理解:</p> <ul style="list-style-type: none"> •收集策略、技术和工具。 •网络情报/信息收集能力和存储资料库。 •信息需求和收集要求在扩展的企业中被翻译、跟踪和优先处理。 •需要与网络运营规划相关的智能规划产品。 •网络运营规划计划、战略和资源。 •网络操作策略、资源和工具。 •网络操作概念、术语/词汇 (即环境准备、网络攻击、网络防御)、原则、能力、限制和效果。 	
	<p>个人 (选手) 应具备的能力:</p> <ul style="list-style-type: none"> •使用适当的策略, 创建的优先级别, 通过收集管理过程 (collection management process) 进行数据收集 (Execute collection)。 •支持收集网络犯罪或者外国情报机构证据活动, 减轻可能的实时威胁, 应对间谍和内部威胁、外国破坏行动、国际恐怖组织活动, 或者为情报活动提供支持。 	
8	调查	15
	<p>个人 (选手) 需了解和理解:</p> <ul style="list-style-type: none"> •威胁调查、报告、调查工具和法律/条例。 •恶意软件分析的概念和方法。 •收集、打包、传输和储存电子证据的过程, 同时并维持监管链。 •司法流程, 包括事实陈述和证据。 •持久性数据的类型和集合。 •数字取证数据的类型和识别方法。 	

	•网络安全漏洞的具体操作性影响。	
	个人（选手）应具备的能力： •通过一系列调查工具和流程，为高级人员的工作提供支持，包括但不限于访谈和审讯技术，监视，反监视和监视检测。 •收集、处理、保留、分析和展示计算机相关的证据，网络弱点的减轻措施，和/或犯罪、欺诈、反情报、以支持司法部门的调查。	
合计		100

3.竞赛项目

本次选拔赛由第三方承办，以第 47 届世界技能大赛网络安全项目为指导，并结合世赛标准和国内行业实际来组织命题。只考核技能部分，不涉及理论。

（一）竞赛内容

竞赛为技能实操，涉及信息系统环境安全加固模块、夺旗行动（CTF）挑战模块 2 个部分。

（二）赛题难度

本次竞赛难度等级应等价（包含）于以下认证水平：

- Certified Information Security Professional：注册信息安全专业人员（CISP）
- Cisco Certified Network Associate (CCNA) Security：思科认证网络工程师（CCNA）安全；
- Microsoft Certified Solutions Expert (MCSE): Desktop Infrastructure:
- 微软认证解决方案专家（MCSE）:服务器架构
- Advanced Level Linux Certification LPIC-2 or equivalent skill set:
- 高级 Linux 认证 LPIC-2 或等效技能

3.1 竞赛模块

表 3.1.1 竞赛模块

模块编号	模块名称	时间分配	分值权重
A	信息系统环境安全加固	3 小时	50%
C	夺旗行动（CTF）挑战	3 小时	50%
总计		6 小时	100%

3.2 模块简述

3.2.1 模块 A

信息系统环境安全加固模块。该模块中，选手需要根据《信息安全管理体系标准（ISO27001-2013）》和等级保护相关标准，对目标操作系统和网络环境进行安全加固与配置。针对 windows 操作系统，主要涉及到 windows 系统账号安全、服务安全、权限分配及数据安全等；针对 linux 操作系统，主要涉及账户安全、登陆安全、访问控制、文件权限等方面；针对基础网络设备，主要涉及交换机的登陆安全、密码安全、端口安全、流量镜像、VLAN 划分、网络防环、静态路由、动态路由、路由协议的认证安全、ACL 访问控制、防火墙不同区域配置和对区域间流量的控制策略，以及实现分部私有网络对总部私有网络的有效访问。主要考察选手对信息技术风险管理标准、政策相关规定和要求的理解和把握能力，对 windows 和 linux 操作系统的脆弱点进行相应安全配置的实际操作能力，以及对路由器、交换机和防火墙等基础网络设备的安全配置、管理和运维能力。

3.2.2 模块 C

夺旗行动（CTF）挑战模块。该模块中，选手被指派去获取对应目标中的 flag 并提交到平台得分。本竞赛模块分成五个任务，必须在规定的时间内完成规定任务，并进行充分的测试，确保获取到的 flag 是正确的。Flag 可能来自于一台远端

的服务器，一个复杂的软件，也可能隐藏在一段通过密码算法或协议加密的数据，或是一组网络流量及音频视频文件中。选手需要综合利用自己掌握的安全技术，并辅以快速学习新知识，通过获取服务器权限，分析并破解软件或是设计解密算法等不限定途径来获取 **flag**。夺旗行动（CTF）挑战中，队伍成功提交一道题目的 **Flag** 即可得到相应的分数（分数会在题目信息中体现），分数会实时体现在队伍的积分榜中。队伍的积分相同时，按照提交最后一个 **Flag** 的时间排序，最先提交 **Flag** 的队伍排在前列。

本模块中，赛题类型分为 **WEB**、**MISC**、**CRYPTO**、**PWN**、**REVERSE** 五大类别。

夺旗行动（CTF）挑战模块名词介绍	
类型名称	类型内容介绍
Web	题目会涉及到常规的漏洞及部分渗透测试相关性题目
MISC	安全杂项，可能涉及流量分析、各种网络取证、社会工程学、数据分析等类型
CRYPTO	密码学，考察各种加解密技术，算法等
PWN	常为溢出类题目
REVERSE	逆向工程，主要涉及到软件逆向、破解等技术

3.3 命题方式

本项目竞赛题的命题方式：本项目为可以提前公布样题的项目。所命竞赛题的内容基于第 47 届世界技能大赛的技术要求，赛前 1 天裁判长可结合赛场设备、材料状况，按照本项目试题调整的工作流程和方法，组织裁判人员对已公布的试题进行不超过 30% 的修改、调整。然后，由裁判长对最终比赛试题审核确认。调整后的竞赛试题不再重新发布。

3.4 命题方案

赛题设计要求：

- 赛题参考世界技能大赛该项目进行设计，模块的命题符合世界技能大赛的基本要求。
- 评分点的设计上，每个模块评分点在 50—80 个之间，单个评分点分值不高于 0.1 分，不要高于 2 分。

4.评分标准

4.1 测量评分

测量评分打分方式：按各模块评分表设置若干个评分组，每个组所有裁判一起商议，在对该选手在该项中的实际得分达成一致后最终只给出一个分值。测量分以测试功能或查看配置情况来评分，测量分只有两种结果，即得分和不得分。

测量分评分准则样列表：

表 4.1.1 评分标准表

子项 ID	子项名称或描述	评分细则	正确分值	得分值

样例：Web Server(windows 2018)

表 4.1.2 评分标准表样例

子项 ID	子项名称或描述	评分细则	正确分值	得分值
A1	Web Server(windows 2018)	IIS 服务监听在 TCP 的 443 端口	0.2	0.2
		配置 IIS 支持 ASP.NET 4.5	0.1	0.1
		设置安全审计策略	0.3	0

4.2 评分流程说明

竞赛开始的前 1 天，各参赛队伍按照裁判长的安排进行裁判分工，裁判长根据裁判员人数和评分工作量对裁判员分工。每个裁判只对裁判长分配指定的对应模块及指定的评分项进行评分，评判的过程完全按照评分标准进行评分。

为确保评分过程的公平性和公正性，评分过程采取回避制度，裁判执裁过程中不能与自己的选手有任何交流，评分过程中不参与自己选手的评分。无相应模块（评分项）执裁任务的裁判不得进入选手工位，不得干扰和影响其他裁判的执裁工作。

4.3 统分方法

各模块裁判员完成本模块指定评分项所有参赛选手评分后，对本人本模块（评分项）评判结果进行核对确认。裁判长对总成绩复核，并将参赛选手成绩交本参赛队裁判员，各裁判员最终签字确认本参赛队选手成绩后，由工作人员录入系统。

4.4 裁判组构成和分工

4.4.1 裁判组

裁判组共 5 人，由 1 名裁判长、4 名裁判员组成。裁判长由第三方技术指导专家担任，裁判员由参赛队所在学校分别选派一名指导教师担任。裁判长可指定一名助理，协助裁判长工作，但不参与评分。裁判长对于技术要求、考核办法、评分标准等有最终解释和裁决权。

4.4.2 裁判任职条件

- 1) 热爱祖国，遵纪守法，爱岗敬业。有较强组织协调能力和团队合作精神。

身体健康，有足够时间和精力投入到世赛工作。

2) 从事本专业技术工作 5 年以上，有高级技师职业资格或副高级以上专业技术职称或相对应的行业技术等级证书，或专业技能高超，得到行业普遍认同。

4.4.3 裁判分工方案

本项目的裁判由裁判长进行分工，裁判必须严格按照执裁流程和裁判岗位内容完成执裁工作，包括相关竞赛技术性文件学习。在执裁过程中需要全程参加整个执裁和评分过程，包括赛前的准备工作，场地、设备准备与检验，竞赛试题的调整与试做，评分标准的制定与确认，选手进场的抽签，执裁过程中的监督与问题处理，评分，竞赛成绩的汇总、审核、确认等。

5.竞赛相关设施设备

5.1 每工位设备清单

表 5.1 工位设备清单

序号	设备名称	型号	单位	数量
1	服务器	1、CPU:3.7GHz, 4.5GHz Turbo 2、内存: 32G 3、存储: 固态硬盘+2TB 3.5 英寸 SATA (7,200 Rpm) 硬盘	台	1
2	台式机	CPU: 酷睿 i5-9500, 6 核, 9MB 缓存, 3.0Ghz 内存容量: 8GB 2666 MHz DDR4 固态硬盘: 512G 机械盘: 1 TGB USB: 4 PCI: 1 视频接口: HDMI/DP 网卡: 1000Mbps 以太网卡 电源: 260W 电源功率: 260W	台	2

5.2 软件技术平台

表 5.2 软件列表

序号	软件名称	版本	单位	数量
1	VMWare vSphere ESXi	Version6.7	套	1
2	VMWare vSphere Client	Version6.0	套	1
3	VMware Workstation	Version16.0.0	套	1
4	Windows Server 2018		套	1
5	Windows 10 Enterprise		套	1
6	Linux(CentOS)	Version7.6	套	1
7	Metasploit Framework			1
8	Kali		套	1
9	Cuckoo sandbox		套	1
10	Splunk		套	1
11	WAF mod_security	Version2.9.3	套	1
12	Snort NIDS/NIPS		套	1
13	Wireshark		套	1
14	OSSEC	Version2.8.1	套	1
15	Tripwire		套	1
16	IDA free		套	1
17	MySQL	Version5.7.25	套	1
18	Winhex	Version19.7	套	1
19	Nmap	Version 7.60	套	1
20	Apache TCPMon	Version1.0	套	1
21	Radare		套	1
22	OllyDbg	Version1.10 &Version2.01	套	1
23	Volatility	Version2.6	套	1
24	Autopsy	Version4.10.0	套	1

注：最终工具列表以赛场实际环境为准。

5.3 场地禁止自带使用的设备和材料

本次比赛选手不能携带任何设备和材料进入比赛现场。

6.项目特别规定

项目特别规定用于提供该项目所特定的一些细则，并明确各项目在竞赛中不同的地方。项目特别规定包括但不限于：个人 IT 设备、数据存储设备、因特网接入、程序和工作流程、文档管理和发放。

表 6.1 项目特别规定

项目/任务	项目特别规定
使用技术—个人照相机	裁判—任何情况下，不得携带个人照相机进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准。 选手—不得将照相机带入场地，直至竞赛结束。
使用技术—移动设备	裁判—任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长批准。 选手—电子设备（包括移动电话）必须存放在选手背包中（关机或静音）放于储物柜中。任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准。
资源文件/笔记	选手—任何情况下，不得携带笔记进入竞赛场地。在选手竞赛场地工位中记录的笔记必须竞赛期间全程都留在选手桌上。不得将任何笔记带出竞赛场地。
设备故障	选手—如果出现设备故障，选手必须立即举手通知裁判。裁判应将选手因故障不能操作的时间记录在案。如果设备故障导致的时间损失，将在模块的规定时间之外给予补时。 如果设备故障前未能存盘导致的时间损失，不予补时。
最终的测试项目	选手—所有选手的最终的测试项目将进行备份，而且在竞赛总结时提供给选手。

7.赛场布局要求

根据本项目的特点，比赛场地包含了选手竞赛区、技术支持区、裁判工作区、休息区。各区域配置基本的设施，场地布置和安全等方面参照世界技能大赛相关要求，赛场的每个工位都必须被现场摄像头拍摄到。

8.健康安全

（一）选手安全防护要求

- 1) 参赛选手应严格遵守设备安全操作规程。
- 2) 参赛选手停止操作时，应保证设备的正常运行，比赛结束后，所有设备保持运行状态，不要拆、动硬件连接，确保设备正常运行和正常评分。
- 3) 参赛选手应遵从安全规范操作。
- 4) 参赛选手应保证设备和信息完整及安全。

（二）选手禁止携带物品

- 1)任何储存液体、气体的压力容器；
- 2)任何有腐蚀性、放射性的化学物品；
- 3)任何易燃、易爆物品；
- 4)任何有毒、有害物品；
- 5)任何没有生产厂商或达不到国家安全标准的工具及设备；
- 6)任何可能危及安全问题的物品；
- 7)任何影响竞赛公平性的物品。
- 8)考核方案禁止携带的物品。

（二）赛事安全要求

1) 承办单位应设置专门的安全防卫组，负责竞赛期间健康和安​​全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

2) 赛场应具备良好的通风、照明和操作空间的条件；赛场需留有安全通道，必须配备灭火设备；

3) 赛场须配备相应医疗人员和急救人员，并备有相应急救设施。

4) 选手、裁判和相关工作人员​​的防疫工作按组委会要求执行。

9.绿色环保

（一）环境保护

环境整洁卫生，体现绿色环保，严格遵守竞赛规则，提高安全意识和卫生意识，遵守职业规范。

所有竞赛相关人员必须保持场地整洁。交通路线、走廊、楼梯、紧急疏散通道、灭火器及其他救生设备周边必须保持畅通无障碍，竞赛结束后，选手要整理好竞赛工位的卫生，赛场保洁人员要保障赛场整体的环境卫生，体现安全、整洁、有序，将垃圾分类处理。

（二）可持续性

竞赛项目设计和筹备工作要遵循可持续发展原则，耗材回收有序，设备循环使用。工位将被用于为相对应的模块进行测试。为了减少网络设备的数量，工位设备将用于多个模块的测试环境，使用技术手段进行快速轮替。