

## 附件4：驻场技术服务要求

### 一、校园网运维服务区域

包含重庆工程职业技术学院所有室内和室外场所，以及协议期内校区内新建建筑场所。

与校方管理人员一起整合运维服务资源，规范运维行为，确保服务质效，形成统一管理、集约高效的一体化运维体系，保障校园网络和应用系统安全、稳定、高效、持续运行。

### 二、常规驻场技术服务要求

序号	服务内容	服务要求
1	主要要求	为确保重庆工程职业技术学院校园网相关设备完好，运转正常，由中标方联合比选一家运维公司配备本次专项驻场服务，并依据 ITIL V3 流程管理体系，以 ITSS 理念为基础，以质量交付为中心的 IT 运维管理要求，为校方提供驻场服务。
2	校园网资产管理服务	(1) 驻场人员对校园网设备、机柜、光纤配线、信息点等进行摸底，整理资产清单，绘制网络及设备动态拓扑图。 (2) 对校园网 IP 资源网格、列表等视图方式对 IP 地址资源进行网格化分配和管理，在动态拓扑图上通过颜色、图标标识 IP 使用属性和状态。
3	监测及巡检服务	(1) 驻场人员每日对校园网络设备、机房等设备进行日常巡检工作，巡检设备的各个指标状况，巡检完成后形成巡检报告，并按校方要求时间节点提供巡检报告报告。 (2) 对校园网络拓扑中的线路和设备实时监测：包括资源名称、端口信息、连接信息、链路类型、性能指标、信息指标、告警数量等。其中设备的信息指标包括：资源名称、IP 地址、MAC 地址、持续运行时间、设备说明等。 (3) 设备的性能指标包括：CPU 平均利用率、内存利用率、Ping 时延等；链路的信息指标包括：链路名称、链路说明、链路类型、链路带宽；链路的性能指标包括：带宽利用率、上行带宽利用率、下行带宽利用率、上行流量、下行流量、广播包率、丢包率、单播包率、组播包率、错包率等。 (4) 对校园网络接入设备实时监测，发现网络中的 IP 地址，计算网段的容量、使用率、在线 IP 数；实时修改发现接入设备的 IP 地址、MAC 地址、所属网段、上联设备名称、上联设备接口。

4	故障处理服务	<p>(1) 提供对故障诊断排除服务，保证校园内各种网络设备稳定运行。协议期内提供设备保修服务，在授权的范围内协调产品供货商予以维修，并监督维修过程和质量。学校原有网络设备（保修期外）故障设备处理，应及时定位故障点，在授权的范围内配合校方协调做好维修，更换故障配件工作。</p> <p>(2) 按照要求进行硬件设备普查工作，检查硬件设备实际运行情况，设置硬件设备及运维档案库。</p>
5	备份与恢复	<p>(1) 对关键的网络设备服务配置文件进行定期离线备份；</p> <p>(2) 根据信息中心实际应用情况、根据生产相关数据的连接关系、根据应用的业务特点和软硬件资源，制定详细的系统数据备份计划，确定合理的系统备份策略。定期备份重要配置信息及数据信息等；</p> <p>(3) 按照控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；</p> <p>(4) 按要求，定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；</p>
6	网络安全管理服务	<p>(1) 对机房主机、网络设备和应用程序的运行状况、网络流量、用户行为等进行监测和报警，形成记录、妥善保存并按重要性级别，进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；</p> <p>(2) 指负责网络运行日志、网络监控记录的日常维护和报警信息分析和处理工作，提出优化建议及方案；</p> <p>(3) 根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；</p> <p>(4) 定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；</p> <p>(5) 定期检查违反规定上网或其他违反网络安全策略的行为，并形成书面报告；</p>

### 三、高级驻场技术服务要求（原厂工程师）

服务项	服务内容	服务描述
高级技术支撑服务	技术咨询服务	<p>1.针对核心网络设备相关产品和技术问题，可以快速为校方和中标方提供专业的解答，要求原厂驻场人员精通相关产品和技术</p> <p>2.为其它驻场工程师提供技术咨询服务，指导其它驻场人员完成信息搜集、分析判断、处理故障。</p>
	疑难复杂问题处理	<p>1.针对校园网运维过程中的疑难复杂问题，能够快速分析判断并给出解决方案。</p> <p>2.针对于跨多产品，涉及多种技术或不明确问题范围的技术故障能够主动快速组织原厂相关产品的技术专家人员，形成专家小组联合诊断并消除故障。</p>

	升级研发处理	针对于非常规性问题，涉及到产品和协议底层的问题，以及协议对接问题，能够主动快速协调厂家相关研发人员介入，通过底层分析来进行深入定位。
网络主动优化服务	网络优化服务	对客户现有网络的基础架构、技术架构、业务流量承载、基础服务能力等各方面情况进行综合评估分析，结合客户的业务部署及发展需求，分析客户网络的运营及支撑能力能否达到业务的运营及发展要求。同时依据现网状况和业务需求的分析结果，对架构规划、协议规划、配置参数、安全加固等内容提出优化建议。
	网络健康检查服务	能够借用原厂多种系统管理工具，对校园网设备进行主动健康检查，及时发现问题并提供解决方案或优化方案。
	版本升级推荐	结合现网软件版本情况以及市场同版本迭代情况，适时对校园网设备软件版本进行推荐，确保校园网设备运行稳定的软件版本，避免已知问题或高风险问题发生
网络设备风险预警与升级	产品软件风险预警	及时总结厂商的软件版本预警通告，结合校园网实施应用场景和配置，判断是否匹配相应的风险，并及时告知解决或规避
	版本升级推荐	结合现网软件版本情况以及市场同版本迭代情况，适时对校园网设备软件版本进行推荐，确保校园网设备运行稳定的软件版本，避免已知问题或高风险问题发生。
	典型风险事件及解决方案推送	针对于典型的风险事件（如勒索病毒、协议漏洞、护网行动等）及时向学校推送相关事件和解决方案，避免出现同类的风险事件

#### 四、驻场技术服务人员要求

服务内容	服务描述
驻场运维服务	<p>1. 中标方提供不低于3人的驻场运维服务，服务人员应包含本次校园网设备制造商原厂技术工程师至少1名，普通网络工程师不少于2名，服务时间8年5*8的驻场服务，7*24小时应急服务。</p> <p>2. 原厂驻场人员能力要求：（1）理论水平具备真实CCNP或行业内同等证书；（2）具备主流厂家数通、无线、安全产品规划实施和故障处理能力；（3）具备较强沟通和项目管理能力；（4）具有良好的团队合作能力，良好的文档编写能力；（5）对技术有很强烈的兴趣，喜欢钻研和学习；（6）良好的沟通表达能力和职业操守，能严格自律；自我学习能力强，善于思考和分析问题。</p> <p>3. 原厂驻场服务团队组成不限于：一名现场驻场服务人员、省区技术专家产品技术专家、重大故障专项专家团队。</p> <p>4. 其它驻场人员能力要求：技术过硬，熟练掌握各类硬件、软件、网络等方面技术，能够自主提供技术服务，及时处理常见技术故障。遇到自身不可解决的故障，应具备调集外部技术支持的能力，以尽快解决故障。</p>

	5. 中标方派遣的驻场服务人员必须政治可靠、作风扎实、遵纪守法、服从校方管理，遵守校方的工作纪律和要求并与校方签订《保密责任书》。
--	-------------------------------------------------------------------

## 五、服务报告提交要求

根据第二条服务内容及要求，定期提供书面报告。

序号	报告	报告方式	频度
1	事件处理报告	格式文档（邮件）	事件发生时
2	设备巡检报告	格式文档（邮件）	每日
3	月工作报告	格式文档（邮件）	每月
4	季度服务报告	格式文档（邮件）	每季度

## 六、技术培训服务

为学校信息中心管理老师提供网络技术培训服务，对所出现的软件操作、软件故障、硬件故障等问题，及时整理汇总，每一季度对出现问题进行统一培训，防止类似问题多次发生，以免影响科室工作进度。

## 七、停机维修时限

如需停机维修必须提前确定停机时间，并报校方人同意，具体要求如下：

- 1.预计停机时间不超过 5 分钟的，须口头征得校方同意。
- 2.预计停机时间超过 5 分钟不足 1 小时的，须提前 1 天征得校方书面同意。
- 3.预计停机时间超过 1 小时的，必须提前 2 天向校方提交书面申请，征得校方书面同意后进行。
- 4.所有需停机的维护必须安排在非工作时间（晚上 10 点至次日凌晨 7 点）进行，并在确定的停机时间内恢复系统正常运行。

## 八、用户档案记录及知识库建立

通过在使用过程中的发现的问题和处理方案的整理汇总形成档

案，有利于统一的不断修改优化，使系统的功能得到持续完善，系统的性能不断提升，运行更加稳定。

在本项目维护服务期限内，中标方需要求驻场人员为用户建立项目运维知识库，并纳入运维知识库模块的规范管理中，本项目知识库主要包括项目文档、以及针对日常维护相关的设备维护常识、设备特性、使用经验、常见故障处理等内容，完善项目运维知识库，形成本项目运维知识体系。

现场服务知识库管理体系包括描述、跟踪知识的录入、审核、发布、更新、运用及删除等生命周期过程的管理流程。

为了保证知识库管理体系长期稳运行和维护，中标方需指定专人负责知识库的管理制度、办法的制定及监督、执行，是知识库的归口管理部门，并设置知识库管理专员。

## **九、服务响应时间**

需要中标方针对本项目提供服务响应承诺，7×24 小时全天响应，驻场人员服从校方调配，并完全按照校方情况安排工作时间，保证 5×8 小时工作日制，节假日提供 7×24 小时远程监控及电话支持服务或者服从校方另行安排

根据优先级启动应急预案：

当系统发生一、二级故障，须立即进行响应，并启动预先制定好的应急方案，在 60-90 分钟内使系统恢复进行，且必须立即安排专业技术人员对故障进行处理，影响系统可靠性时间每次不能超过两小时。

当系统发生一般性故障，必须在 1 小时以内有实质性响应，影

响系统可用时间每次不能超过 4 小时。

故障等级	故障等级描述	驻场人员响应时间要求
一级故障	影响校园网业务系统全部功能	及时响应，工作日 5 分钟内到达故障现场，非工作日 40 分钟到达故障现场。90 分钟内排除故障,恢复系统正常运行或启用。
二级故障	影响校园网业务关键功能	及时响应，工作日 5 分钟内到达故障现场，非工作日 60 分钟到达故障现场。120 分钟内排除故障,恢复系统正常运行或启用。
三级故障	影响校园网业务部分功能	及时响应，工作日 15 分钟内到达故障现场，非工作日 1.5 小时内到达故障现场。当日排除故障，保证系统恢复正常运行
四级故障	一般设备故障	及时响应，工作日 20 分钟内到达故障现场，非工作日 2.5 小时到达故障现场。当日排除故障，保证系统恢复正常运行。

## 十、保密政策与保密协议

校方涉及的所有相关资料（网络拓扑图、IP 地址、技术方案、密码、网络安全设备配置等）和数据均为保密材料。中标方应该遵照国家相关规定按照保密要求进行项目工作，并采取相应的保密措施。

必须按照国家有关法律的要求，采取有效的保密措施，保证资料的安全，未经允许不得带出、不得向第三方提供。

协议到期后，中标方不得保留任何与该项目有关的数据以及基于数据开发的任何成果。

未经校方审阅和许可，中标方不得发表于该项目有关的技术报告、论文和广告宣传图片，也不得进行公开的传媒报道与宣传。

## 十一、网络安全事件处置

1.及时报告所发现的安全弱点和可疑事件，但任何情况下均不应尝试验证弱点；

2.在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，提供防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。

（以下无正文）