五、 服务承诺

（一）技术方案承诺

1、 服务目标

等保测评目标：完成 6 个核心系统的二级等保备案、测评、差距分析及整改指导，顺利取得备案证明和合格的等保测评报告，确保所有系统符合《信息安全技术 网络安全等级保护基本要求》及等保 2.0 二级标准要求。

驻场运维目标：构建全流程的校园网安全运营体系，实现校园网基础设施、操作系统、机房硬件、网络安全设备的规范化运维，保障系统全年稳定运行，故障响应及时、处置高效，杜绝重大安全事故和长时间业务中断。

风险评估和加固目标：每年完成一次全校业务系统的全面风险评估，精准发现安全漏洞和管理隐患，完成针对性加固整改，提升校园网络安全应急处置能力，完善安全管理制度体系，增强全校师生和技术人员的网络安全意识与实操能力。

整体安全目标：通过三年系统化的安全服务，建立学校网络安全长效保障机制，实现安全资产可管、安全威胁可测、安全事件可控、安全风险可防，全面满足学校信息化建设的安全需求。

2、 质量承诺

建立三级审核机制：工程师自审→项目经理复审→技术总监终审，测评报告一次通过率 100%，整改后复测通过率 100%。

所有服务均严格遵循国家信息安全等级保护 2.0 标准、《信息安全技术 网络安全等级保护基本要求》及学校的相关要求，确保服务质量符合“合格”标准，满足采购人需求。

我公司所有资质证书均在有效期内，服务人员具备项目要求的专业认证证书和工作经验，上岗前进行专项培训，确保具备完成项目服务的专业能力。

建立服务质量三级复核机制，项目负责人对服务过程和成果进行一级复核，部门经理进行二级复核，技术总监进行三级复核，确保所有服务成果准确、规范、完整。

针对等保测评备案时限、故障响应时间、二线工程师到场时间等关键指标，

建立专项考核机制，若未达到要求，按合同约定承担相应的违约责任，确保项目工期和服务效率。

服务期内持续收集学校的反馈意见，建立服务改进台账，针对问题及时制定整改措施，持续优化服务流程和服务内容，提升学校的服务满意度。

3、 合规承诺

所有测评工具经公安部认证，测评方法符合《网络安全等级保护测评要求》，严格按照 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等保 2.0 标准执行。

4、 保密承诺

建立数据分级分类管理制度，核心数据采用加密传输和存储，签订专项保密协议，所有接触数据人员签署保密承诺书。

服务期内，我公司签订保密协议，我公司承诺严格保护用户系统、数据、信息的安全，在服务期满后永久不得泄露用户所有信息。由于我公司违反保密协议而导致的泄密或破坏，由我公司负全责，并由我公司赔偿用户所有损失。我公司提供服务期内保护用户系统、数据、信息的安全，以及服务期满后永久保守用户信息秘密的承诺书。

（二） 时间安排承诺

1、 等保测评-时间安排

序号	时间	内容
1	第 1-3 天	项目启动会→资产梳理→定级材料准备
2	第 4-7 天	差距分析初测→问题清单整理→整改方案制定
3	第 8-15 天	整改实施（同步进行）→复测准备
4	第 16-20 天	等级测评复测→报告编制→专家评审
5	第 21-25 天	报告修订→备案材料整理→公安报备
6	第 26-30 天	取得备案证明→项目验收→资料移交

2、 等保测评-关键里程碑控制

序号	时间	内容
1	第 7 天	完成差距分析报告提交
2	第 15 天	完成整改实施并具备复测条件
3	第 25 天	完成备案材料提交至公安机关
4	第 30 天	取得备案证明，项目验收

3、 驻场运维服务（三年）

本服务采用“1 名驻场 HCIP 工程师+二线专业技术团队”的服务模式，驻场工程师同步学校作息时间，实行 5×8 小时现场服务+7×24 小时全天候响应，二线团队提供 4 小时现场到达、24 小时非硬件故障解决的技术支撑，全面覆盖校园网全维度运维需求，服务期内持续构建校园网安全运营体系。

1.团队配置与资质要求

驻场工程师：计算机相关专业本科毕业，具备 2 年以上相关工作经验，持有 HCIP 证书，熟悉网络设备、安全设备、服务器、存储、虚拟化、数据库等运维管理操作，严格服从学校网络管理部门的管理和考核。

二线服务团队：成员持有路由交换方向 IE、服务器与存储方向 IE、OCM 数据库方向认证、VCP 虚拟化认证、信息安全保障人员证书等核心证书，团队为驻场工作提供全流程技术支撑。

我公司具备 ITSS 信息技术服务标准符合性二级认证证书，确保运维服务的规范化、标准化。

2.核心运维服务内容实施

（1）安全资产治理（服务期全程）

进场后 10 个工作日内，完成校园网服务范围内资产的全面梳理，涵盖操作系统、数据库、中间件、应用系统的版本、类型、IP 地址，应用开放协议和端口，应用系统管理方式、资产重要性及网络拓扑等信息，按学校格式要求整理归档并交付校方。

建立资产动态管理机制，资产发生变更时，第一时间跟踪、确认并更新信息，

确保资产信息的准确性和时效性。

协助学校制定并维护安全资产静态基准，创建符合等保要求的信息系统安全基线，搭建系统黄金镜像库、安全软件版本库、安全系统配置库。

（2）漏洞和补丁管理（每月定期开展）

制定标准化的漏洞和补丁管理计划，每月对校园网所有资产进行安全状态检查，精准发现系统脆弱点和漏洞。

严格按照管理流程和测试流程，对漏洞进行分级处置，完成补丁的安装和修复，修复前充分与学校沟通，避免影响业务正常运行，所有操作均留存记录。

（3）变更管理（按需开展）

制定完善的资产配置变更管理计划，针对学校提出的合理变更需求，进行深度技术分析、测试和验证。

按流程发起变更申请，变更完成后及时更新安全配置基线，持续优化资产静态安全性，确保所有变更操作可追溯、无安全隐患。

（4）威胁监测和处置（7×24 小时实时开展）

基于学校威胁监测和分析平台，实时监测和分析网络流量，及时发现攻击行为、漏洞利用等安全威胁。

对发现的安全漏洞进行人工分析验证，结合威胁情报信息，判断威胁程度和影响范围，排查可疑主机，协助学校开展安全加固，持续跟踪整改情况，形成闭环处置。

（5）安全事件响应（7×24 小时待命）

协助学校建立规范的安全事件响应规范，制定针对性的响应流程和操作脚本手册。

基于威胁监测和态势感知平台，对安全数据和日志进行关联分析，及时发现安全事件并通知校方，协助开展通报、处置工作，优先恢复业务，消除或减轻事件影响，事后出具书面故障处理日志和分析报告。

（6）全维度基础设施运维（每日开展）

虚拟化运维：对虚拟化基础设施、私有云组件进行日常监控、技术支持，记录运行数据，及时排查故障。

操作系统运维：提供操作系统安装、配置、加固、故障排除服务，确保系统稳定运行。

机房硬件运维：每日对中心机房硬件设备进行健康巡检，排查故障，协助处理设备保修事宜，记录巡检和故障数据。

网络和安全设备运维：对网络和安全设备进行日常管理、策略调整、配置优化，确保网络传输安全、通畅。

3.响应机制与故障处置

基本响应：采购人发现问题或巡检发现问题后，1 小时内完成问题级别、影响范围、解决资源、解决时长的初步判定，立即开展故障排查和处理。

二线现场响应：接到校方二线工程师现场支持请求后，4 小时内工程师到达现场，非硬件故障 24 小时内解决；系统遭遇灾难性崩溃时，二线工程师 8 小时内赶赴现场，全力开展系统恢复工作。

重大事件响应：校园网发生故障、重大事件或学校举办重大活动时，派遣专业工程师现场不间断服务，直至系统恢复正常，满足学校业务需求。

4.日常管理与文档交付

人员管理：驻场工程师 5×8 小时在岗，不得临时更换或长期脱岗，如需更换需提前征得学校同意，严格遵守学校各项管理制度，接受学校网络管理部门的考核、监督和评价。

巡检管理：驻场工程师每日对所有设备进行现场巡检，检查物理运行环境、系统运行状态和系统日志，每日向网络管理部门汇报巡检情况。

文档管理：建立完善的系统维护档案及日志，按日、周、月出具运维日报、周报、月报，内容涵盖巡检情况、故障处理、设备变动等；留存校园网设备巡检日志、软硬件配置变动日志、故障处理日志等所有运维记录，定期交付学校归档。

增值支持：配合学校及校园网管理部门，为学校各类活动、信息化建设提供技术咨询和建议；协助完成新增设备与原有设备的集成互联互通工作；按学校安排提供网络运行相关劳务支持。

5.培训服务（服务期内 4 次）

建立技术交流和培训机制，根据学校需求提供本地或异地培训，每次不少于

1 人参加。

培训内容兼顾理论和实际操作，涵盖校园网日常运维管理、紧急故障处理办法、新技术介绍、软硬件基础知识等，确保学校技术人员能够独立开展运维管理、应对和处理各类紧急故障，熟练操作机房内运维安全设备。

4、 风险评估和加固服务（三年，每年 1 次）

本服务每年开展 1 次全流程的风险评估、安全加固、应急演练、培训和制度咨询，我公司具备信息安全风险评估二级、信息系统安全运维二级、信息系统安全集成二级资质证书。

1. 安全评估

全面风险评估：对学校所有业务系统的应用系统、操作系统、部署位置、安全域划分、安全设备防护等进行全方位评估，发现安全隐患并提出解决建议。

运维管理评估：对核心资产的密码、日志、版本信息、安全策略等进行检测，识别管理层面的风险点，形成整改建议。

威胁分析：过滤分析网络流量，及时发现危险行为、攻击目标和攻击方式，对重点目标进行风险判断，提供针对性防护建议并协助处理。

主机安全检查：检测重点主机是否存在木马、后门等恶意程序，分析系统日志，排查入侵痕迹。

人工验证：对所有漏洞和威胁信息进行人工验证，杜绝误报，完成后出具《网络安全风险评估报告》和《系统整改建议书》，交付学校。

2. 安全加固

补丁加固：针对评估发现的系统补丁漏洞，在与学校充分沟通并进行必要测试后，完成补丁安装和漏洞修复。

配置参数加固：对权限设置、策略配置、参数设置等配置类问题进行优化加固，确保系统配置符合安全规范。

安全管理加固：针对组织、人员、安全域规划等管理层面的风险，提出完善建议并协助学校落地实施。

加固整改完成后，对整改效果进行复核，出具《整改加固报告》，详细说明所有整改项目的实施情况和效果。

3.网络安全应急演练

制定贴合学校实际的应急演练方案，模拟网络拥塞、病毒入侵、网站被攻击等常见安全事件。

组织学校相关工作人员按照《网络安全事件应急响应指南》完成事件上报、处置全流程操作，规范响应流程，提升处置及时性。

演练结束后，对演练过程进行复盘分析，总结问题并提出优化建议，出具《安全演练工作报告》。

4. 应急响应服务

学校发生网络安全事件时，服务团队第一时间响应，协助解决问题、查找事件原因、提出加固建议并协助完成加固。

上级机关开展安全检查或学校收到上级/公安机关安全通报时，提供全程技术支持，协助学校完成整改工作。

每次应急响应结束后，出具《应急响应报告》，记录事件处置过程、结果和后续防护建议。

5.安全培训服务

技术人员培训：面向学校信息化技术人员，讲解常见网络攻击类型、安全日志分析方法、安全软件使用、应急响应和处置思路，结合实际案例开展实操教学。

全员安全意识培训：面向全校师生，介绍网络安全常见风险、个人和单位防范措施、常用安全技巧，提升全校师生的网络安全意识，降低安全威胁发生概率。

6.制度咨询服务

安排专业安全顾问对学校网络安全建设现状进行实地调查和摸底，协助学校完善网络安全领导机构设置、规章制度制定和办事流程优化。

为学校提供全套网络安全培训教材和案例辅助材料，解读等保政策和行业安全政策，制定信息安全建设规划和蓝图设计，提供信息安全实践方法建议。

（三） 人员配备承诺

1、 核心人员配备表

序号	本项目任职	姓名	证书名称
1	项目负责人	张晓光	信息系统项目管理师（高级）、VMware VCP工程师证书
2	技术负责人	刘小坤	网络规划设计师（高级）、CISP认证
3	驻场工程师	王绍	华为HCIP路由交换方向认证
4	技术工程师	王继富	数据库OCP级别认证、信息安全保障人员认证-风险管理（专业级）
5	技术工程师	王宏宇	华为HCIE路由交换方向认证、华为HCIE服务器与存储方向认证、信息安全保障人员认证-风险管理（专业级）
6	技术工程师	韩杨	VMware VSP工程师证书、信息安全保障人员认证-风险管理（基础级）
7	技术工程师	周水东	VMware VCP工程师证书
8	安服负责人	刘西洋	数据库OCP级别认证、数据库OCM级别认证、CISSP认证工程师证书
9	安服工程师	马豪杰	CISP认证
10	安服工程师	周之翔	CISP认证

2、 人员配备保障

（一）组织架构保障

成立专属的项目服务团队，设置项目负责人（统筹全项目服务工作，对接学校高层管理部门）、驻场运维负责人（由驻场 HCIP 工程师担任，负责日常运维工作）等，团队成员均为专职人员，明确岗位职责，确保各项服务有序开展。

（二）制度流程保障

建立项目服务管理制度，涵盖人员管理、服务流程、质量考核、保密管理等方面，确保服务标准化、规范化。

制定服务沟通机制，每周与学校网络管理部门开展一次工作沟通会，汇报服务进展、问题处置情况，收集学校需求和意见；重大问题第一时间上报，及时制定解决方案。

建立服务质量考核机制，接受学校的全程监督和考核，根据考核结果持续优化服务工作，若服务质量未达要求，按学校要求及时整改。

（三）保密管理保障

服务期内，与学校签订正式的《保密协议》，所有服务人员均签订个人保密承诺书，严格遵守保密约定。

建立数据和信息保密管理制度，对学校的系统数据、业务信息、运维记录等所有信息进行严格保密，所有电子资料设置加密保护，纸质资料专人保管、专柜存放。

承诺服务期满后永久不泄露学校任何信息，若发生泄密行为，按合同约定承担全部责任，赔偿学校所有损失，情节严重的依法追究相关人员法律责任。

（四）投诉处理保障

设立专属的客户投诉渠道（含投诉电话、邮箱），7×24 小时受理学校的服务投诉。

建立投诉处理流程，从受理投诉到向学校初次回复处理意见不超过 8 小时，以问题解决和学校满意为投诉处理终点，处理时限不超过 15 个自然日，所有投诉均留存处理记录。

若因服务质量、人员管理等问题给学校造成重大影响，按合同约定向学校支付赔偿金，并按学校要求撤换相关人员、改善服务质量，直至满足学校需求。

（四） 与相关单位的配合方案承诺

1、 配合方案机制

配合对象	配合内容	配合方式
新乡职业技术	系统访问权限、业务协调、	每日站会、每周周报、紧急事

配合对象	配合内容	配合方式
学院	整改实施	项即时沟通
公安机关（网安部门）	备案材料提交、测评报告审核、备案证明获取	指定专人对接，提前预审材料，确保一次通过
系统开发商/集成商	技术细节确认、整改技术支持、漏洞修复协助	建立技术对接群，重大问题现场会商
硬件设备厂商	设备策略优化、固件升级支持、备件协调	签订技术支持协议，开通绿色通道

2、 项目沟通制度

- 问题及早提出准则

对自己承担责任的工作，必须及时发现不能完成的因素，并及时向项目经理或有关责任人提供书面报告，否则不能完成任务的责任将完全在于任务的责任人。

- 及时澄清准则

对所承接的工作，如没有提出拒绝，则代表接受人已经完全了解工作环境、工作要求等多个因素。如果在呈交结果时，与任务要求有偏离，则不可以以任何理由解释责任，失败责任完全在于接受人。因此，接受人应及时与任务分派人澄清任务的全部因素。如果，任务分派人未能及时提供澄清，而造成工程损失的，责任完全在于任务分派人。

- 报告方式

报告必须以书面方式提交。如报告人认为口头报告即可，可采用口头报告，但是如果口头报告没有使问题得以解决，则视同报告人没有提交报告。

3、 沟通管理计划

日常沟通：微信/钉钉工作群，即时响应。

正式沟通：每周五提交《项目周报》，每月提交《项目月报》。

里程碑沟通：关键节点召开正式会议，形成会议纪要。

紧急沟通：重大问题 30 分钟内电话通报，2 小时内现场会商。