晋中学院数据中心运维服务合同

JZZ-2022-HT24

甲方：晋中学院

乙方：山西合力创新科技股份有限公司

服务合同

甲方：晋中学院

乙方：山西合力创新科技股份有限公司

乙方在山西中经招标代理有限公司组织的数据中心运维服务采购项目（项目编号：1499002022CCS01564）采购中成交，经双方协商一致，签订本合同。

一、服务条款

乙方向甲方提供数据中心运维服务。

服务项目	服务实施方	数量	单价（元）	合价（元）	服务期
数据中心运维服务	山西合力创新科技股份有限公司	1	406,800	406,800	一年

（具体服务内容、技术参数等见附件一《服务清单》）

二、合同总金额

人民币（大写）：肆拾万零陆仟捌佰元整

（小写）：406,800 元

三、支付方式

1、本合同总金额为一年的运维服务费；

2、合同签订三个月后，甲方支付乙方合同总金额的 50%（即：贰拾万零叁仟肆佰元整），合同期满甲方考核合格后支付剩余的 50%（即：贰拾万零叁仟肆佰元整）。

四、服务期限及地点

1、服务期限：1 年（从二〇二二年九月一日起至二〇二三年八月三十一日止）。

2、服务地点：甲方指定地点

五、甲方的义务

1、及时办理付款手续。

2、负责提供服务所需的现场环境，为乙方现场服务人员提供工作便利。

3、负责协助乙方完成需求调研工作及项目相关的协调工作。

4、及时组织进行各项目确认工作。

5、对合同条款及价格负有保密义务。

六、乙方的义务

1、保证所提供服务均为响应文件承诺内容，符合相关服务质量标准。

2、乙方应遵守国家有关保密的法律法规和行业规定，并对合同履行过程中的学校、师生个人等各种信息和资料负有保密义务，且不得擅自删除和转移机房系统中的信息。

3、乙方保证对甲方的系统在使用年限内按维护规程所规定的有关标准及附件所规定的要求进行维护，保证其正常运行。

4、乙方工作人员在提供服务期间非因甲方及其人员原因遭受人身伤害、财产损害或侵犯甲方、第三人相关权利的，由乙方承担全部法律责任及赔偿责任。

5、乙方维护更新的软件，不得侵犯第三人的专利权、商标权或工业设计权等知识产权，如有违反，由乙方承担全部法律责任及赔偿责任，给甲方造成损失的，乙方应全额赔偿。

6、乙方应根据甲方要求，及时更换不合格的驻场工程师。

7、乙方不得在未征得甲方同意前终止、拒绝、拖延履行合同约定的服务内容。

8、乙方应遵守甲方关于校园管理和疫情防控的相关要求，并承担不遵守相关要求所带来的一切不利后果。

七、违约责任

1、甲方无正当理由拒付合同款的，甲方向乙方支付合同总金额 2%的违约金。

2、乙方所提供服务质量不符合合同约定标准的，乙方向甲方支付合同总金额 2%的违约金，甲方有权解除本合同。

3、乙方逾期提供服务时，每逾一天乙方向甲方支付合同总金额 3‰的违约金。逾期超过 30 天，甲方有权解除本合同，给甲方造成的损失由乙方承担赔偿

责任。

八、不可抗力

甲、乙双方的任何一方由于不可抗力不能履行合同时，在不可抗力发生后一周内向对方通报不能履行或不能完全履行理由；在取得有关机构证明以后，允许延期履行、部分履行或者不履行合同，并根据情况可部分或全部免予承担违约责任。

九、争议解决

甲、乙双方在履行合同中发生争议，应通过协商解决；如协商不成，可以向甲方所在地人民法院提起诉讼。

十、合同生效及其他

1、合同由甲、乙双方盖章，法定代表人（或委托代理人）签字后生效。

2、本合同一式陆份，甲方持肆份，乙方持一份，采购代理机构存档一份。

3、合同履行过程中出现的未尽事宜，甲、乙双方在不违背合同和招标文件的前提下协商解决，协商一致，达成《补充协议》，与本合同具有同等效力。

十一、下列文件为本合同的必要组成部分

1、竞争性磋商文件

2、响应文件

3、磋商供应商所做的其他承诺

（以下无正文，为本合同签字盖章页）

甲方（章）：晋中学院

法定代表人（签字）：

（或委托代理人）

地 址：晋中市榆次区文华街 199 号

电 话：0351-3985689

开户银行：

账 号：

合同签订地点：晋中学院

乙方（章）：山西合力创新科技股份有限公司

法定代表人（签字）：

（或委托代理人）

地 址：山西综改示范区太原学府园区南中环街 529 号清控创新基地 A 座 8 层 0801、0802、0811-0814 室

电 话：0351-7243701

开户银行：中国光大银行太原双塔西街支行

账 号：75260188000012883

日 期：2022 年 8 月 31 日

附件一：　　服务清单

（一）服务人员及服务团队

1．为保障数据中心整体运维服务服务质量，要求乙方提供固定一线维护服务人员 2 名、在重要节日、关键会议、重要事件等应急期按照学校要求增加 1-2 名运维服务工程师提供服务，完成现场保障和实时监测服务。

固定驻场现场保障工作要求：

（1）日常驻场保障时间为 7*10 时。

（2）驻场人员在办公室驻场，接听维修电话，监视系统运行情况，并做好维修维护记录，形成日志存档。

（3）负责数据机房的安全巡检，驻场人员进行机房巡查时，检查并记录签字，如发现故障、问题或隐患，及时报告学校相关人员，并提出解决方案。

（4）履行驻场职责，确保维护信息设备正常运行，并及时处理各类故障，对于小型配件及耗材（货物单价≤2000 元）由乙方提供。

（5）驻场人员每日至少在下列时间内巡视数据机房并形成巡检报告：早 8:30-9:00;下午 17:00-18:00。

（6）驻场期间，出现紧急情况应按操作规程立即处理，同时上报学校主要负责人。

2．服务工程师具体要求如下：

（1）一线驻场运维工程师（驻场人员）：

为保障服务质量，乙方提供固定一线维护人员 2 名。

（2）二线运维服务工程师：

1）虚拟化工程师：1 名；

2）网络工程师：1 名；

3）数据库工程师：1 名；

4）信息安全工程师：1 名；

5）服务项目经理：1 名。

（二）现场服务工作开展

为了确保学校数据中心整体服务质量，要求乙方能够有效的依托运维管理支撑平台对数据中心内所有服务工单进行闭环管理，能够灵活的运用安全服务工具开展现场工作。具体现场服务工作内容和如下：

1、基础架构运维

1.1 资产维护

乙方对学校服务范围内的信息资产依据服务动态进行实时更新，记录在资产统计表中，包括服务器、网络设备、存储、机房安防设备等，记录资源情况。其中通用资产更新范围要求如下：

（1）数据中心硬件资源：服务器、存储、网络设备、安全设备等；

（2）软件资源：操作系统、数据库、中间件等；

（3）应用软件资源：业务应用系统；

（4）设备主要配置项：用户名、密码、主机存储硬件配置文件、网络设备配置表；

（5）IP 资源：现网 IP 资源使用情况。

除此以外，为了满足国家网络安全等要求，在资产梳理和更新过程中，还要针对学校现有各类应用业务和主机，依托安全服务工具箱重点实现如下内容：

（1）能够通过搜索引擎或者字典文件猜测可能存在的域名，并对一个网段进行反向查询，可启用递归查询，可设置 WHOIS 请求之间的时间延迟；可允许用户指定输出位置；

（2）获取目标主机的系统信息：IP 地址、系统时间和主机名等信息；

（3）工具通过分析数据中心的数据包，对数据中心主机上的操作系统进行鉴别，主要识别的信息：包括；操作系统类型、端口、是否运行于防火墙之后、是否运行于 NAT 模式、是否运行于负载均衡模式、远程系统已启动时间、远程系统的 DSL 和 ISP 信息等。

1.2 计算环境运维

计算环境是学校业务承载的关键平台，整体运维工作包括硬件服务器集群、虚拟化软件平台等。针对这些软硬件开展日常的巡检、例行维护、故障处理、现场监护、性能优化等工作。

1.2.1 硬件集群维护

（1）日常巡检

每日对服务器进行日常巡检服务，巡检工作通过两个方面开展，现场服务人员要通过观察服务器硬件指示灯等方式获取硬件运行状态，查看设备系统运行情况，是否有报警和故障。

服务器健康检查(服务器运行环境、操作系统和系统安全、服务器操作系统、服务器运行固件版本、硬件运行情况、设备连接状态、供电情况、补丁及固件维护兼容性检查、系统日志、系统时钟同步等)。

通过运维监控平台对整体服务器硬件集群运行状态进行监控和展示。

通过运维监控平台对整体集群高危故障进行实时告警,告警形式不限于企业微信、邮箱、微信等。

(2) 例行维护

数据中心服务器提供维护配置故障处理服务,对托管服务器进行监控管理服务。

安装系统或程序的补丁、对重要数据的备份、对服务器 IP 地址规划。

服务器台账更新及维护:能形成电子资产台账,方便学校进行查阅,台账涉及资产编号、服务器名称、序列号、品牌型号、CPU、内存、硬盘、业务系统、IP 地址、操作系统、机房编号、机柜位置、起始 U 位、结束 U 位、网卡数量、HBA 卡数量、存储空间、维保信息、安装日期、责任人。

各服务器分区日志信息检查,主要包括操作系统告警日志,计划任务执行日志等信息。

各服务器分区资源使用情况检查,主要包括 CPU 使用率,内存使用率,换页空间使用率,文件系统使用率等信息。

服务器高可用信息检查,主要指配置了高可用服务的服务器分区之间的高可用状态等信息。

多路径状态信息检查,主要指服务器与存储之间多路径软件的运行状态、多路径状态等信息。

(3) 故障管理

提供设备故障定位服务,辅助定位故障原因并进行故障处理。

在每次处理故障完成后,在 2 个工作日内提交《故障处理报告》,包括故障原因分析、处理过程、维护建议等。

1.2.2 虚拟化平台维护

(1) 软件台账管理及维护(虚拟化版本、集群状态、网络使用情况、IP 信息、用户名、tools 状态、责任人,将所有元素组成虚拟化平台 IT 资产信息配置管理库并进行日常更新维护)。

（2）例行维护

为了提升维护效率，缩短对虚拟化平台维护真空期，利用自动化手段，依托运维监控平台收集私有云平台环境的下关键业务系统资源使用情况、报错情况、监控各虚拟机性能情况，是否存在延迟、空间占用、带宽占用过高的问题。

定期可汇总虚拟化管理日常状态包括：健康状态、群集配置状态、DRS 策略状态。

每周检查虚拟机备份情况，对备份异常的及时处理。

每日检查虚拟机状态启动停止、虚拟机健康状态、虚拟机快照、虚拟机配置（硬盘、网络、IP、主机名）。

每日检查虚拟化平台网络状态：分布式交换机标准交换机日常维护、配合测试网络链路状态、虚拟化管理端口与虚拟机业务网络连通性。

虚拟化平台存储状态：存储映射状态确认，存储微调配合支持。

针对学校业务系统上线正常运行提供支持配合。

虚拟机日常维护操作（虚拟机创建、虚拟机开关机、虚拟机系统安装、虚拟机快照创建、虚拟机备份等）。

按照学校要求对虚拟机进行备份计划，备份执行情况维护。

虚拟化平台关键业务系统虚拟机正常运行日常维护。

业务虚拟机运行情况(CPU 使用率、内存使用率、硬盘 IOPS 值)的监控。

业务访问高峰期系统资源占用情况进行检测记录。

业务使用中虚拟机报错信息进行收集整理以及业务故障进行协助排错和数据恢复。

对业务应用系统的运行情况进行全面分析和维护。

对虚拟化平台进行规划建议。

（3）故障处理和告警

虚拟数据平台发生故障时，能够及时排查各种故障，能够及时解决虚拟数据平台出现的各种软件故障，保证虚拟数据平台的正常和稳定运行。

乙方能够对虚拟化平台软件故障处理常见故障进行有效的告警和处置，故障类型支持：虚拟化计算资源、虚拟化网络、虚拟化存储，计算服务器故障切换、虚拟机动态资源分配、虚拟化资源动态迁移（更改虚机主机位置和更改虚机存储位置）分布式网络、分布式存储等。同时支持对接企业微信、邮箱、微信等有效

的告警方式，让乙方和学校相关人员能够第一时间收到故障告警信息。

虚拟化平台硬件故障处理，利用虚拟化平台运维工具，监控支撑业务应用的服务器底层硬件指标，虚拟数据平台发生故障时，能够及时排查故障，及时发现并定位造成故障的硬件原因，当用户提供备件后进行安装协助工作，保证虚拟数据平台的正常和稳定运行。

（4）现场监护

在对虚拟化平台服务器、存储、网络做调整时，虚拟化平台运维人员协助进行现场监护。

（5）虚拟数据平台的性能优化

根据业务的访问压力情况，合理地调整虚拟化环境的资源分配策略，解决瓶颈和资源浪费，最合理最大化地利用资源，并避免环境出错；周期性提交优化建议。

1.2.3 租户运行日常管理

★乙方依托运维监控平台，对学校整体计算环境中的各类租户主机进行日常管理，能够支持对 Windows、Linux 类型操作系统的管理，同时能够实时展示对于各租户 CPU、内存、进程、网络流量、磁盘性能的具体数据。

为了降低对计算环境资源的无效消耗，能够通过代理和无代理两种方式对主机性能进行监控；同时支持 IPMI 方式监控服务器硬件，监控内容包括温度、电源、风扇、电压等硬件状态。

1.3 存储维护

（1）日常巡检

每日对存储设备进行日常巡检服务，主要指通过观察存储硬件指示灯等方式获取硬件运行状态，查看设备系统运行情况，是否有报警和故障。

存储健康检查，需要对接运维监控平台，具体包含指标如下：

检查设备运行物理环境；

电源电池供电情况；

关键部件（硬盘、控制器、驱动器等）运行状态；

光纤线路连通性；

网络链路连通性等设备环境；

IO 读写效率；

系统事件日志等信息。

（2）例行维护

存储台账更新及维护（资产编号、存储类型、存储名称、序列号、品牌类型、管理地址、服务地址、容量、机房编号、机柜位置、维保信息、安装日期、固件版本、配置 Raid 信息、存储池、维护厂商、责任人）。

存储常规配置、容量规划、日常映射。

核对和备份 SAN 交换机配置信息，并保存备份数据。

核对校验存储和交换机设备微码，多路径软件版本。

核对校验存储逻辑卷读写性能。

存储设备管理系统的日志检查。主要包括磁盘阵列、NAS 设备管理控制台的运行相关日志。

SAN 交换机硬件及端口状态检查，主要指通过观察 SAN 交换机设备及各端口指示灯等方式获取硬件运行状态。

磁盘容量使用情况检查，主要包括存储未分配容量、已分配容量、已分配未使用容量等信息。

SAN 交换机日志信息检查，主要包括 SAN 交换机端口日志信息和设备日志信息等。

（3）故障处理

提供设备故障定位服务，辅助定位故障原因并进行故障处理。

在每次处理故障完成后，在 2 个工作日内提交《故障处理报告》，包括故障原因分析、处理过程、维护建议等。

1.4 环境安全监测

（1）服务范围

1）对数据中心机房(含学校东西汇聚机房、电池间)内部基础设施的资源，包括 5 台制冷设备、配电系统、3 套 UPS 系统资源资产监测服务。

2）对全校 104 个竖井环境安全、消防安全监测巡检。

3）对中心机房基础设备运行(服务器、存储等硬件设备)监测。

4）对机房整体环境(温湿度、机房卫生情况)巡检监测。

5)梳理晋中学院数据中心内部基础环境的资源，记录在资产统计表中，包括制冷设备、门禁系统、监控系统、配电系统、UPS 系统等基础环境设备的运行情

况，明确设备间的依存关系，建立台账并及时更新；建立学校、校内用户和设备供应商的关系接口，明确各方职能边界，保障服务质量。

（2）服务内容

1）日常巡检

机房基础设施(空调、UPS、配电、门禁等)运行状态进行巡检监测记录；

机房环境、温湿度进行巡检监测记录；

机房基础设备(服务、存储、网络设备等)运行状态巡检监测记录；

通过动环软件系统对全校竖井环境进行监测记录。

在每次处理故障完成后，在 2 个工作日内提交《故障处理报告》，包括故障原因分析、处理过程、维护建议等。

2）每日对机房环境进行清理、整理、除尘等工作。

3）每月对中心机房、东西汇聚机房、电池间进行大型清扫服务并形成书面记录。

4）每两周至竖井现场查看竖井环境、消防情况并做巡检记录。

5）每季度对竖井环境进行清扫、整理、除尘等工作。

6）负责维护竖井内环境安全监测设备保证正常运行。

7）根据学校要求对机房实施必要的优化调整。

8）日常巡检发现的问题记录在《巡检报告表》中，并汇报网络信息中心。

9）提供设备故障定位服务及基础环境设备故障处理服务，确保服务范围内涉及的设备和系统能够稳定可靠运行。确保服务范围内涉及的设备和系统能够稳定可靠运行。

10）在每次处理故障完成后，在 2 个工作日内提交《故障处理报告》，包括故障原因分析、处理过程、维护建议等。

11）协助学院对设备内容进行维护，包括记录和更新设备维修、维护和变更信息等。

12）负责强弱电线路、插头等插牢、插紧。

13）进入机房的人员进行登记，并监督其活动情况。

14）定期提供机房空调外机清洗工作（寒暑假）。

2 网络运维

2.1 数据中心网络运维

对以太网网络交换机和SAN网络交换机例行安全巡检。内容包含：基础配置情况、流量监测、CPU负载、内存负载、端口状态、ARP监测，巡检结果记录至《日巡检报告》中。

能够将相关运行参数对接到运维监控平台，通过该平台对异常运行情况进行告警。

配置管理服务：检查配置信息，完成每月配置备份；网络结构发生变化时，按照晋中学院网络信息中心要求修改配置信息、系统口令、权限等。网络系统升级优化服务：对设备安全策略、访问控制列表、路由策略的调整；进行设备软件系统升级、消缺；对设备性能进行分析、进行配置调优。

故障管理：驻场人员收集故障信息，定位故障原因，找到对各类常见故障的解决办法，形成较为完善的各类问题解决方案。

2.2 校园网络运维

对校园网络2台H3C12508核心交换机、4台H3CS7506E汇聚交换机、2台H3CS7503E数据中心交换机、1台H3CS7506E网络出口交换机、405台48口接入交换机、65台24口接入交换机以及相关网络连接件、18615个数据点，969个数据配线架,202个光纤配线架等现有网络设备、线路、接入点、连接件进行运维。

运维费用包括除核心交换机、汇聚交换机、接入交换机等设备以外，其他网络综合布线系统维护、运营所需的配线架间跳线、办公室跳线更换、网络水晶头、数据配线架等一切材料设备。

（1）工单响应及处理服务

提供维护区域每周7*10小时用户工单现场处理服务，按照事先确定的故障等级和用户类型提供不同的服务级别。

服务台负责完成工单的生成、派发、处理、回访、关闭等操作，做到100%的响应率和处理率，对每件工单形成闭环管理。

运维人员依照知识库标准答案或查询相应信息数据库进行答复，服务台无法回答或处理的问题生成工单，转派给一线、二线人员或学校相关部门。

（2）网络系统硬件及链路维护服务

1）确保网络的接入设备连接正常，如相关设备存在可用性故障，能够及时告警，并推送相关告警信息到运维人员及管理人员；

2）对网络设备的修复（设备修复的原因：设备损坏、光模块损坏、链路老化）在尽可能短的时间内完成，尽快恢复网络的传输；

3）对区域新上硬件设备进行安装调试，保障网络正常运行；

4）对学校各类网络设备进行日常监控，能够支持对设备 CPU 利用率、内存利用率、端口状态、端口出入流量、Ping 延时、丢包、错包等指标进行实时展示；

能够构建学校实时网络运行的动态拓扑图，可动态展示设备运行状态；同时能够自动发现新接入设备，检测类型包括：SNMP、TCP、HTTP、ICMP、Telnet 等，可自定义更新间隔、检测 IP 范围等；

5）对每个报障电话，需有详细记录，每周需提供用户故障分析报告、每月提供运维服务报告、巡检报告、每年提供年度总结报告发给网络信息中心相关人员；

6）负责竖井、配线间、室内所有交换机的更换；

7）针对网络链路和接口等校园网问题的事件进行及时处理；

8）人员变动导致线路变更或 MAC 变更，对变更信息的统计并协助用户完成 IP-MAC 地址的绑定和相关数据库录入工作；

9）出现大范围内的设备故障或重要部门、核心设备故障时，快速提出解决方案，并做出人员调配和应急措施。

（3）主动巡检服务

定期对交换设备巡检，并提供巡检报告报告。

（4）二线支持服务

负责提供对一线支持人员无法解决的疑难网络问题进一步进行调研分析，找出解决方案并尽快恢复服务，二线支持主要工作：

1）完成疑难网络事件深入调查和分析；

2）根据经验和专业技能，决定需要采取何种措施恢复服务并实施有效的行动；

3）及时协调厂商三线技术支持；

4）提供有效故障解决方案。

（5）重大事件应急保障服务

在重大会议、重要事件、突发情况等特殊时期，提供工程师在岗服务，以保障学校信息安全。特殊时期的保障服务包含：

1）校方举行重大活动或重要事件时，增加运维工程师驻场进行现场的网络保障；

2）学校有大范围的网络改造或者业务系统测试等项目，安排高级技术工程师进行现场的配合工作。

3 安全服务

为学校提供专业的安全服务，服务期内综合运用学校现有安全组件，提供资产安全管理、安全评估、脆弱性管理、威胁管理、安全问题响应处置、安全培训、安全意识宣传等个性化安全服务。

3.1 安全设备运维服务

（1）日常巡检

每日对数据机房安全设备进行巡检工作，查看设备硬件运行情况，包括电源状态、风扇状态、端口状态、设备出口温度等。

（2）保障内容

1）设备基本情况：设备性能基本参数、设备电源、设备保修状态及运行的版本情况、软件包、规则库、当前时间等，并保持各安全设备规则库为最新；

2）设备外围：设备外观、指示灯状态、电源风扇、散热、灰尘、连接线缆情况完整度等情况；

3）运行日志：着重对日志中的警告、错误、阻断等类型日志进行检查和分析，对已发送的问题进行统计汇总，并预测；

4）设备口令情况：对设备口令进行巡检，杜绝弱口令的使用，同时按照密码管理规定，对过期口令进行清理；

5）设备用户情况：对设备用户情况进行巡检，确保设备用户架构满足三权分立原则，对设备用户不安全登陆情况进行巡检；

6）设备规则情况：对设备中的规则情况，访问控制策略进行巡检，并进行备份；

7）设备负载：对设备在巡检周期内的负载情况进行巡检，按照使用周期整体负载情况，给出扩容升级和维护建议。

8）资产识别与梳理：乙方借助安全服务工具箱对招标方资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性。

乙方结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、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、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。

9）事件管理：基于主动响应和被动响应流程，对页面篡改、通报、断网、Webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案。

实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。

针对分析得到的勒索病毒、挖矿病毒、篡改事件、Webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助招标方快速恢复业务，消除或减轻影响。

入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。

入侵威胁清除：排查攻击路径，恶意文件清除。

入侵原因分析：还原攻击路径，分析入侵事件原因。

加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。

10）故障处理

提供 7*24 小时电话支持服务，在接到故障报修后的 10 分钟内响应，并在不超过 24 小时对安全设备故障进行修复。

3.2 安全现状评估

乙方工程师在入场后，对学校整体安全状况进行一次全面评估，评估方式灵活，工程师可携带安全服务工具箱，对以下方面进行评估，内容包括但不限于以下内容：

系统与 Web 漏洞扫描：对操作系统、数据库、常见应用/协议、Web 通用漏洞与常规漏洞进行漏洞扫描。

弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、MsSQL、MySQL、Oracle、smtp、VNC、ftp、telnet、ssh、MySQL、tomcat 等。

基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基

线配置情况，确保达到相应的安全防护要求。检查项包含但不限于账号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况。

蠕虫病毒事件：需确认文件是否被感染，定位失陷的代码并进行修复。

针对漏洞利用攻击行为、Webshell 上传行为、Web 系统目录遍历攻击行为、SQL 注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。

失陷主机分析：需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。

潜伏威胁分析：需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT、C&C 通道、隐藏外联通道等外联威胁行为。

需对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。

3.3 脆弱性管理

在服务期内，乙方为学校各重要业务系统提供脆弱性管理服务，服务如下：

脆弱性扫描与验证：提供不少于每月一次针对服务范围内的资产的系统脆弱性和 Web 漏洞进行全量扫描，并针对发现的脆弱性进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。

优先级排序：提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。

脆弱性验证：提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，安全专家跟进脆弱性状态，各个处理进度透明，方便我方清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化。

修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。

脆弱性复测：需提供脆弱性复测措施，及时检验脆弱性真实修复情况。支持

学校可按需针对指定脆弱性问题，指定资产等小范围进行，降低脆弱性复测时的潜在影响范围。

对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得学校可做到脆弱性的可视、可管、可控。

最新漏洞预警与排查：需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。

最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。

最新漏洞复测与状态跟踪：由乙方对该最新漏洞建立状态追踪机制：跟踪修复状态，遗留情况。

3.4 威胁管理

结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于学校现有安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括脆弱性信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，发现各类安全事件，并能够监测到相关事件，汇总到运维管理支持平台，自动生成工单，快速并自动化协调相关工程师进行处置。

及时对病毒事件进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发 DOS 型、C&C 访问型、文件感染型、木马型。

乙方需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户。

结合威胁情报，乙方需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。

乙方需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒。

乙方需每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置

建议。

乙方需每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置。

乙方需每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务。

策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。

策略定期管理：乙方需每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果。

通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。

通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。

实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。

3.5 安全问题处置和响应

在服务期间，借助安全服务工具箱对发现的安全问题进行现场+线上方式开展处置，对于需要进行现场处置的安全问题，相关工程师需要配备专业服务工具箱开展，具体问题范围包含但不限于：

（1）脆弱性问题处置

针对内网脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建议。

（2）病毒类事件处置

针对病毒类事件。安全专家提供病毒处置工具并主导查杀 10 个实例。若超过 10 个实例，安全专家固化出实际可行的措施，确保用户可进行查杀病毒。

（3）入侵攻击行为处置

针对分析研判确认的入侵行为，安全专家给出策略调整建议。如果有 AF 设备等，在获得授权后，在服务时间内安全专家调整安全策略。

（4）失陷类事件处置

针对勒索、挖矿类事件。安全专家主导处置工作，并提供最大程度溯源服务；安全专家定位恶意文件路径并提供查杀指导；并分析有无异常进程与服务，发现异常进行通告。

针对后门脚本类事件。安全专家主导处置工作，提供专杀工具对感染服务器

进行全面后门脚本查杀，并提供最大程度溯源服务。

针对隐藏通信通道、可疑外发行为。安全专家提供实际佐证材料，并给出修复建议，提供最大范围的溯源服务。配合定位异常进程以及恶意文件，并提供查杀建议。

（5）漏洞管理

利用漏洞扫描工具扫描网络中的核心服务器、重要的网络设备以及WEB业务系统，包括服务器、交换机、防火墙等，以对网络设备进行安全漏洞检测和分析，对识别出的能被入侵者用来非法进入网络或者非法获取信息资产的漏洞，并将这些漏洞信息与业务资产信息通过漏洞管理平台进行统一关联、展示与追踪，使得管理人员可以有效地追踪业务资产漏洞全生命周期，实现漏洞信息全生命周期的可视、可控和可管。

通过利用学校部署的漏洞扫描工具，并按照一定的安全策略进行扫描，扫描完成后，触发处理相关流程，具体要求如下：

组件部署：设置定时定期对内网主机、系统进行安全扫描，扫描结果安全运营中心；

漏洞识别与分析：安全专家对漏洞工单进行确认并进行优先级排序；

修复方案：安全专家提供处置建议及方案，通知相关处理人员；

安全加固：现场人员处理，并同步处理结果到安全运营中心；

跟踪复测：安全运营中心开启漏洞复测流程，确认漏洞是否成功修复。

（6）威胁通告

结合威胁情报，安全专家排查是否对学校资产造成威胁并通知用户，协助及时进行安全加固。

最新漏洞通告与响应。

资产指纹信息梳理：梳理信息化资产详情（含操作系统、中间件、数据库、应用框架，开发语言等指纹信息）并将梳理的信息录入安全运营平台。

最新漏洞预警与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。

最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。

（7）数据库安全加固

从身份鉴别、访问控制、安全审计、入侵防范、剩余信息等多方面对运维范围内业务系统的数据库按照三级等保的要求进行安全加固，形成安全加固报告，并定期对数据库进行漏洞扫描和更换密码，对发现漏洞及时提供解决方案并和学校进行充分沟通，安排检修窗口及时消除安全隐患。

3.6 安全培训

在服务期内，为了提升网络信息中心工作人员及校内师生整体安全意识，要求乙方在服务期内为学校按需提供安全意识培训，同时在必要时期（如国家网络安全宣传周）协助学校开展网络安全宣传，具体如下：

协助学校开展安全意识培训，培训内容包括但不限于：常见安全漏洞原理、复现与防范、内网渗透、权限维持与防范、社会工程学等。

安全宣传周要求协助学校制作符合国家网络安全宣传主题的各类宣传资料，包括但不限于宣传视频、易拉宝、宣传海报、宣传资料彩页等。

4 统一数据库运维

运维范围内数据库包括：数字化校园平台数据库、数字化校园业务数据库等数据库，以及服务期内数据中心为新上线业务系统建立的数据库或者数据模式。

数据库系统出现故障、运行过程中有技术疑问需要技术咨询或学校重要业务保障期，学校可随时拨打由乙方提供的一、二线服务热线电话，电话支持级别一年 365 天全天候服务支持，乙方应立即处理客户的电话请求，按照故障级别提供必要技术支持与诊断、故障处理直至客户得到满意的结果。

对学校数据库专责人员进行 ORACLE 数据库运维技能培训，培训结合数据库软件环境进行，能够理论和实战结合，培训结果确保学校运维人员具备日常巡检，问题处理，性能分析的能力，并且熟练使用各种运维工具。

4.1 数据库台账收集及动态维护

梳理目前在用数据库运行架构，收集现有数据库运行详细信息，形成数据库台账，并随配置变更和运行情况变更进行及时维护。

4.2 巡检

一线服务工程师每日现场对运维范围的数据库进行技术巡检，检查数据库可用性、存储使用情况、性能情况、健康情况、非法对象情况、任务执行情况、备份执行情况、热备环境可切换性、冷备可恢复性等多方面，发现问题及时处理并

记录生成日巡检报告，问题及时交给二线处理和跟踪。

结合数据库运行情况，每月对数据库运行情况、检修情况、配置变更情况、问题处理情况、故障恢复情况、安全加固情况等多方面综合进行分析，形成运行月报。在长期运行数据积累的基础上明确各数据库系统日常巡视基础平台系统的KPI并脚本化，建立数据库系统运维基线。

乙方为学校提供一体化的数据库运行维护工具，建立个性化的运维服务体系，实现数据库运维工作有序化。结合实际情况，搭建ORACLEEMCLOUDCONTROL平台，对所有数据库进行统一运维和监管。

4.3 数据库升级

乙方应安排工程师对服务期内所维护的数据库软件在正常使用过程中可能触发软件BUG，或者发现安全漏洞，提供临时性补救措施，并安排计划检修进行软件升级与补丁操作。

在现有数据库基础上，上线安装或者部署新的业务系统或者功能模块时，根据业务系统厂商要求，结合网络信息中心对数据库用户、账号、表空间、权限管理要求，进行表空间规划，权限规划和创建，辅助数据库高可用和负载均衡连接串配置，协助进行数据导入等工作，业务系统上线前进行全面的SQL审核和数据库性能测试，提供测试报告，并协助应用软件厂商进行优化改进。

4.4 全面数据库健康检查及隐患排除

乙方定期（每季度一次）指派高级工程师到达用户数据库软件使用现场，对数据库软件运行状况进行全方位无死角的信息系统隐患排查及整改服务，排查范围应从高可用配置、主机配置、操作系统配置、数据库软件配置、备份恢复可用性、性能和运行情况等6个方面开展。及时发现问题并出具健康检查报告，在与学校进行充分讨论沟通后解决问题，安排计划检修窗口对隐患进行逐一消除，将数据库故障风险化解于“未病”阶段。

4.5 数据库性能优化

乙方现场人员及时关注运行数据库性能指标，按需组织力量对数据库进行优化，从操作系统、实例、SQL等多方面进行全面、综合、主动的数据库性能优化，给予业务系统厂商SQL优化指导或使用数据库新特性，满足业务系统使用需求，有效降低资源消耗。

5 其他服务

随着学校资产梳理的快速增加，业务系统的快速普及，网络信息中心需要为师生提供的IT服务也急剧增加，同时中心内部各类IT事件的发生频率也快速增加，在这种情况下，要求网络信息中心能够对所有现场支持的事件处置进行有效的调度并进行闭环管理，这样才能有效提升对各类IT事件的响应效率，并监督处置结果、改善处置过程、决策资源配置。乙方需要具备相关能力，才能有效支持学校现有服务需求和现状，具体对乙方的现场活动管理要求如下：

（1）★能够对接网络信息中心报障电话，对电话咨询和报障进行有效管理。

（2）★能够灵活对接服务入口，如电脑端、手机端，学校企业微信等多种渠道，要求无需繁琐的文字描述即可实现故障上报。在处理过程中，可以上传必要的文字、照片、视频记录。

（3）能够对其工程师的故障处理情况、处理过程、巡检等进行有效的可视化管理。

（4）能够对学校整体运维工作进行通过各类图表，进行整体的实时数据展示。

（5）能够带动网络信息中心及相关技术人员形成技术讨论的氛围，对于维护故障处理经验、方法和解决方案进行积累。并能够全员参与对知识条目进行点赞，回复等社区交流活动，培养学校整体技术氛围。

（6）支持满意度调查及满意度评价功能。

乙方协助网络信息中心开展服务的满意度调查，能够提供主动电话回访调查和移动端消息通知调查和统计。

（7）对全年服务开展情况进行统计，包括不限于：工单数统计、平均处理时长统计、工程师故障处理工作量统计、工程师维修处理工作量统计、知识分类统计、贡献量统计。

5.1 应急演练服务

为了提升晋中学院对突发事件的应急响应能力，增强学校参与单位和人员等对应急预案的熟悉程序，加强配合，提高应急处置能力。乙方在服务周期内，配合学校开展应急演练服务1次。

（1）演练原则

结合实际、合理定位。紧密结合应急管理工作实际需求，明确演练目的，根据资源条件确定演练方式和规模。

着眼实战、讲求实效。以提高应急指挥机构的指挥协调能力和应急队伍的实战应变能力为着眼点。重视对演练流程及演练效果的评估、考核，总结推广经验，对问题及时整改。

周密部署、确保安全。围绕演练目的，精心策划演练内容，科学设计演练方案，周密部署演练活动，制订并严格遵守有关安全措施，确保演练参与人员及演练设施安全。

统筹规划、厉行节约。统筹规划应急演练活动，演与练有效互补，适当开展跨行业、跨地域的综合性演练，充分利用现有资源，提升应急演练效益。

（2）演练场景

围绕晋中学院实际业务环境和情况开展应急演练，演练场景包括但不限于：电力故障、网络安全（口令爆破、web 漏洞遏制、恶意程序遏制）、服务器节点故障、数据库存储故障、核心网络故障、ESXi 主机网络端口异常、虚拟化上联交换机故障、FC 交换机故障、存储双活等。

（3）演练要求

应急演练工作分为演练准备、演练实施、演练总结和成果运用四个阶段。

演练准备阶段是确保演练成功的关键。包括制定计划、设计方案、方案评审、动员培训、演练保障等几个方面。

演练实施阶段是演练的实际操作阶段，包括系统准备、演练启动、演练执行、演练解说、演练记录、演练宣传、演练结束和系统恢复几个方面。

演练总结阶段是对演练全面回顾，归纳问题和经验，包括演练评估、演练总结、文件归档和备案、考核与奖惩几个方面。

演练成果运用是在演练总结的基础上，对问题和经验的运用，包括完善预案、实施整改、教育培训等。

5.2 值守

（1）值班人员在办公室值守，正常接听维修电话，监视系统运行情况，并做好维护记录。

（2）负责数据中心机房、两个汇聚机房、一个电池间环境的安全和动环巡检。值班人员进行机房巡查时，检查并记录签字。如发现故障问题、或隐患及时报告网络信息中心相关人员。

（3）104 个竖井的动环情况巡检，如发现掉线或警告信息，及时进行处理并

上报。

（4）认证履行值班职责，确保值班期间数据中心正常运行，并及时处理各类故障。

（5）值班人员在上午 8:30-9:00，下午 17:00-18:00 进行数据中心机房巡视，检查并签字记录。

（6）如遇国家重大节假日（两会等）提供 N*24 小时值班服务。

5.3 驻场

为保障数据中心整体运维服务服务质量，乙方提供固定一线维护服务人员 2 名、在重要节日、关键会议、重要事件等应急时期按照学校要求增加 1-2 名运维服务工程师提供服务，完成现场保障和实时监测服务。

5.3.1 固定驻场现场保障工作要求

（1）日常驻场保障时间为 7*10 小时。

（2）驻场人员在办公室驻场，接听维修电话，监视系统运行情况，并做好维修维护记录，形成日志存档。

（3）负责数据机房的安全巡检，驻场人员进行机房巡查时，检查并记录签字，如发现故障、问题或隐患，及时报告学校相关人员，并提出解决方案。

（4）履行驻场职责，确保维护信息设备正常运行，并及时处理各类故障，对于小型配件及耗材（货物单价≤2000 元）由乙方提供。

（5）驻场人员每日至少在下列时间内巡视数据机房并形成巡检报告：早 8:30-9:00;下午 17:00-18:00。

（6）驻场期间，出现紧急情况应按操作规程立即处理，同时上报学校主要负责人。

5.4 小型配件及耗材

在服务期内，运维过程中需要的小型配件及耗材（货物单价≤2000 元）由乙方免费提供。

（三）服务开展辅助支撑平台要求

对于学校运维服务的开展，单纯依靠人力已不能满足数据中心对业务可用性、连续性和安全性的各项要求，为了提升整体运维服务质量，提升数据中心对故障和时间的响应能力，乙方必须有能力利用各类自动化工具或平台对开展日常运维工作，要求乙方具备闭环的服务工单和事件管理能力，能够在服务期内，提供相

应的管理平台和工具，作为辅助学校信息中心对服务事件服务工单进行全生命周期的管理，运维管理支撑平台具体如下：

（1）系统采用B/S架构，无需安装任何客户端软件，通过浏览器即可使用。

（2）系统具备开放性，提供必要的规范接口，能够与企业微信等第三方平台进行对接。

（3）支持PC端、手机端访问，可通过多种渠道进行工单上报、接收、转派、处理等操作。

（4）支持对工程师使用情况进行统计，包括接单、建单、任务创建、任务处理、会议、巡检等内容。

（5）系统具备工作看板大屏展示功能，提供运维服务看板、工程师看板、会议看板。看板支持柱状图、折线图、统计图、列表等多种展现形式，看板数据自动刷新。

（6）支持值班管理，可针对工作日、节假日、休息日以及全部日期设定排班规则，支持自定义单次值班天数、值班人数、值班时段、值班人员等内容。支持自动生成排班表，不同的排班规则以不同的颜色进行区分；支持手工修改每一天的排班人员，排班表支持导出和打印。支持节假日设定，能够自动生成排班统计报表，使用户可以很方便的查看不同排班规则下，每个排班人员的值班天数。

（7）支持通过企业微信、服务台电话、浏览器访问等多种方式进行故障上报。支持服务台电话来电弹屏显示电话相关科室信息，对于未关联的电话支持后台维护和关联操作。系统提供丰富的菜单选择，能够满足日常工单录入的需求，整体使用简便，无需繁琐的文字描述即可实现故障上报。支持故障工单抢接、处理、转派、协助、退回等操作。支持在处理过程中查询检索知识库，并且可通过相关知识快速填充处理过程的表单。支持工单跟踪，可即时了解故障的当前处理状态，支持通过移动端进行催单，工单重派、工单取消等操作。支持在处理过程中对工单复杂度进行调整，并支持对所提供服务的次数进行选择，在处理过程中，可以上传必要的文字、照片、视频记录。工单的处理记录包括处理时长的记录、处理类型的记录、处理人员的记录、处理过程的详细记录、所用耗材的记录（包括耗材的类型、单价、总价）。支持历史工单关联，对于重复上报的、取消上报的、再次上报的相同事件，支持快速工单关联。支持针对工单进行满意度调查，支持满意度快速选择和自由评论。

（四）服务输出物

1．基础架构运维输出物：资产维护输出物、计算环境运维输出物、存储维护输出物、环境安全监测输出物。

《数据中心资产统计表》，报告频率：按需更新；

《机房日巡检报告》，报告频率：每日一次；

《竖井安全巡检报告》，报告频率：每月两次；

《月度运维服务报告》，报告频率：每月一次；

《虚拟化平台月度运维报告》，报告频率：每月一次；

《重大事件处理报告》，报告频率：按需触发，不限次数。

2．网络运维：数据中心网络运维输出物、校园网运维输出物。

《日工作报告》报告频率，每日一次；

《运维服务周报告》报告频率：每周一次；

《月度运维服务报告》，报告频率：每月一次；

《重大事件处理报告》，报告频率：按需触发，不限次数。

3．安全服务输出物

《安全服务运营报告》，报告频率：每周一次；

《事件分析与处置报告》，报告频率：按需触发，不限次数；

《安全通告》，报告频率：按需触发，不限次数；

《综合分析报告》，报告频率：每月一次；

《漏扫报告》，报告频率：每月一次。

4.统一数据库运维输出物

《数据库日巡检报告》，报告频率：每日一次；

《数据库月度运维报告》，报告频率：每月一次。

5．其他服务：应急演练输出物、值守输出物

《应急演练方案及脚本》和《应急演练过程报告》；

《数据中心值班记录》和《数据中心值班报告》。

（五）服务要求

1．驻场工程师需具备良好的服务意识、较强的沟通协调能力、熟悉相关国内主流品牌设备故障的报修程序和资料查询方式。

2．校方认定驻场工程师的能力不能满足实际工作要求的，乙方重新选派驻

场工程师。如果乙方重新选派的驻场工程师仍然达不到实际工作要求的，校方有权终止服务。

3．乙方提供 7*24 小时电话支持服务，在接到故障报修后 10 分钟内及时响应，并在不超过 12 小时对设备进行修复。