渭南市政务服务大厅硬件保障及网络维护服务项目合同

采购人（甲方）：渭南市政务服务中心

供应商（乙方）：联通数字科技有限公司陕西分公司

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等法律法规的规定，甲、 乙双方就渭南市政务服务大厅硬件保障及网络维护服务项目（项目编号：ZCSP-渭南市-2025-00290）事宜，本着平等、自愿的原则， 经多次友好协商，达成以下一致意见，订立本合同共同遵守。

一、服务内容

（一）项目名称： 渭南市政务服务大厅硬件保障及网络维护服务项目 。

（二）服务内容事项：为保障政务服务大厅各类设施设备的正常运行，确保大厅各项工作顺利开展，全面提升政务服务大厅网络与信息系统的安全性、稳定性和可靠性，建立健全网络安全防护体系，提升政务服务大厅网络运维水平及应急处置能力，对所有设施设备及网络与信息系统运行维护和安全服务进行服务保障，提供驻场服务及7x24 小时电话响应服务，对政务大厅软硬件系统及设施设备进行巡检维护、故障响应与修理、备件管理、设备性能优化、技术支持与培训。

具体服务内容：对行政服务大厅、企业服务大厅和中心机关所有设施设备进行维修维护，包括但不限于电视、电脑、抽叫号设备、打印机、桌椅沙发以及其他硬件设施设备等；对行政服务大厅、企业服务大厅和中心机关所有软件系统进行运行巡检维护、数据保障、网络安全、信息服务、应急处置、攻防演练等，包括但不限于LED屏、条屏、抽叫号、电视等系统。

二、技术要求： 符合国家标准、行业标准以及现行技术规范要求，达到合格标准。

三、服务期限

服务完成日期：自合同签订之日起一年。

四、合同价款及付款方式

1.本合同价款人民币¥ 337500.00 元 ，大写： 叁拾叁万柒仟伍佰 元整，该价款为含税价，包含完成本次项目所需的人工费、服务费、管理费、税金等所有费用。

2.乙方指定账户：

开户名称：联通数字科技有限公司陕西分公司

开户银行：中国工商银行西安高新区枫林绿洲支行

开户账号：3700028719020013049

3.付款方式：

（1）付款方式：合同签订后，支付合同总价款的50%；合同签订后半年，经评估服务达到合同要求，支付合同总价款的40%；合同签订满一年后，经验收合格，支付合同总价款的10%。

(2)结算方式：甲方与乙方直接结算，乙方负责在付款前按甲方要求提供增值税发票， 甲方见票付款。

(3)支付方式：银行转账。

五、服务要求

乙方需要制定年度维护计划，建立健全运维台账管理制度，按时对运维情况进行登记，配合甲方不定期的检查，项目维护具体要求如下：

1.记录每次为甲方更换的设备或配件的序列号，确保信息的可靠性和延续性；

2.定期将设备的配置文件、硬件配置和操作系统版本等信息进行归类存档，对于有变动的信息则必须注明存档；

3.乙方给甲方的维护意见需要保存在客户文档中，并跟进甲方的工作进展情况以及意见实施后的运行状况；

4.每次故障的处理都需要有详细的记录，便于双方查询。

5.对网络有重大更改，如：核心设备的更换和升级、影响全局的配置更改等。更改前必须提交详细的施工步骤和应急处理方案，经甲方审核同意后才能付诸实施。

6.乙方安排专人进行驻场值守。上下班时间和甲方工作人员一致。(8:30-12:00；13:00-17:00）。如遇重大任务保障、特殊任务、系统不稳定、高温预警等特殊时期，根据甲方要求进行全天候值守，驻场人员在驻场运维期间，因特殊原因需要更换的，须向甲方发起申请。

7.乙方工作人员每日8:50前完成对两个政务大厅的日常巡检，发现故障及时维修维护，并将结果报告甲方。

8.如遇节假日或重大活动时，乙方应提前一日对大厅设施设备进行巡检维护，确保正常运行。

9.如遇故障复杂，或者维护维修量较大时，乙方应加派工作人员进行处理，确保设施设备及时维护维修完毕。

10.严格履行磋商文件中的采购内容及要求，考核（验收）标准和方法：满足甲方需求及相关行业要求。

六、双方的权利和义务

（一）甲方的权利和义务

1.甲方须保证乙方提供技术服务所需要的适当环境、电力供应及相应的人员配合等条件；

2.被维保设备发生故障，甲方应及时将出现的故障情况通知乙方；

3.甲方按合同要求负责及时对乙方提供的维护保障服务进行审核，对于乙方提交的维护巡检报告及时进行确认；

4.甲方有权根据本合同所约定的内容及标准，在不影响乙方工作的前提下检查乙方提供的服务质量，如乙方提供的服务质量不符合本合同的约定，甲方有权要求乙方在指定时间内作出补充或修正；

5.甲方应依据本合同规定，按时足额向乙方支付合同价款；

6.甲方应积极配合、协助乙方完成本合同约定事项。

（二）乙方的权利和义务

1.乙方必须按合同约定的服务内容及标准向甲方提供相应服务；

2.乙方对本合同委托范围内的技术服务的完整性以及内容负责；

3.乙方应配合甲方进行设备、系统的故障排查，甲方有权决定故障最终解决方案；

4.乙方应依据国家有关法律法规的规定进行相应技术工作；

5.乙方有权要求甲方按时足额支付合同费用；

6.乙方应本着节约节俭原则，加强对设施设备的日常维护，减少故障发生。对出现的故障应先进行维修，无法维修或者维修价值不大时，应当及时向甲方提出更换相关配件的建议。

7.甲方负责采购购买相关配件、设施设备，也可委托乙方代购，代购前费用需经甲方确认同意后购买，所需费用由甲方承担。购买后，由乙方负责安装调试，不再另外收取服务费。

8.非工作日期间，甲方需要维护维修设备的，应提前告知乙方，乙方应该于1小时之内到达现场，及时解决问题。

9.乙方在进行电子设备维修时，应提示甲方进行数据、资料转移、备份。乙方可为甲方代做备份。

10.乙方应严格遵守有关数据安全方面的法律法规、规章制度，采取必要措施，防止信息泄露，保障数据安全。

11.乙方必须严格按照合同及响应文件的服务要求，合理安排提供技术服务的进度，高效、及时完成本合同规定的维保服务；

12.如因不可抗力，如恶劣气候或灾害、国家行为等导致服务内容不能如期完成的，乙方应及时通知甲方，由双方另行协商处理；

13.乙方配合甲方进行软硬件升级改造，按合同确定的服务标准承担升级改造后的软硬件维保服务，不再另行收取费用。

14.驻场人员工资、福利及工作产生的一切费用由乙方承担，驻场人员在工作期间产生的以及引起他人的人身、财产损害，由乙方负责。

七、质量保证

乙方所供服务必须执行下列条款：

（一）服务方案和方式科学、可行，人员配置合理，全面满足要求。

（二）符合国家有关服务规范要求，确保各项服务达到最佳效果。

（三）乙方提供的服务，若发生侵权而产生的一切后果，由乙方负责。甲方保留索赔权利。

八、验收

（一）项目最终验收达不到招标文件要求和投标文件承诺及国家或行业标准，或在使用中发现不能容忍的缺陷等，将视为验收不合格，乙方应在规定时间内无条件完善或赔付甲方损失。

（二）若发现乙方有弄虚作假的及在项目实施阶段故意或随意夸大服务，本合同解除，乙方赔偿甲方相应的损失。

（三）验收标准：按照招标文件、投标文件等技术指标进行逐项验收。各项指标均应符合验收标准及要求。

（四）验收合格后，填写验收单，双方签字生效。

九、违约责任

（一）按《中华人民共和国民法典》中的相关条款执行。

（二）未按合同要求提供服务或服务质量不能满足合同要求，甲方有权终止合同，并要求乙方承担违约责任。同时，政府采购监管部门有权依据《政府采购法》及相关法律法规对乙方的违法行为进行相应的处罚。

（三）在本合同履行过程中，双方因违约或造成对方经济、社会效益等损失的应当赔偿。

（四）乙方提供的服务未达到采购需求，按照总价款20%赔偿违约金，并按照合同的内容赔偿甲方损失。

（五）乙方不得擅自将本合同服务转包给第三方承担。

十、保密条款

（一）乙方应遵守国家有关保密的法律法规和行业规定，并对甲方提供的资料负有保密义务。未经甲方同意，不得将承接政府服务项目获得的政府、公民个人等各种信息和资料提供给其他单位和个人。如发生以上情况，甲方有权追究乙方及相关人员的法律责任，并有权要求赔偿因此产生的一切损失。

（二）甲方有义务保护乙方的知识产权，未经乙方同意，不得将乙方交付的具有知识产权性质的成果文件、资料向第三方转让或用于本合同以外的项目。如发生以上情况，乙方有权索赔，但甲方依据相关法定职责对外公开的除外。

（三）本条款为独立条款，本合同的无效、变更、解除和终止均不影响本条款的效力。

十一、知识产权

甲方在中华人民共和国境内使用成交乙方提供的货物及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，乙方应承担由此而引起的一切法律责任和费用。

十二、不可抗力因素

出现下列情况导致本合同不能履行的，双方可豁免违约责任：由于不可抗力（包括疫情、地震、台风、洪水、火灾、战争、罢工、政府禁令以及双方均不可预见、不能控制的事情或　情况）导致本协议不能履行的，合同终止，甲方按履约天数支付乙方相应比例的合同价款，剩余部分价款返还甲方。

十三、争议解决

（一）本合同在履行过程中发生的争议，由甲、乙双方当事人协商解决，协商不成依法向甲方所在地人民法院起诉。

（二）本条款为独立条款，本合同的无效、变更、解除和终止均不影响本条款的效力。

十四、合同变更

在合同的执行期内，双方均不得随意变更或解除合同。如因项目需求情况发生变化，需要项目变更的，应双方协商后签订项目变更协议，双方签字盖章确认后生效（如双方变更事 项不能达成一致的，仍按原合同履行，否则视为违约）。

十五、合同生效

本合同一式 肆 份，甲方持 贰 份，乙方持 贰 份，本合同甲、乙双方签字盖章后生效，合同执行完毕后，自动失效（合同的服务承诺则长期有效）。

十六、其他事项

（一）招标文件、投标文件、澄清表（函）、成交通知书、合同附件均成为合同不可分割的部分。

（二）合同未尽事宜，由甲、乙双方协商确认后签订政府采购补充合同，与原合同具有 同等法律效力。

附件 1：渭南市政务服务大厅硬件保障及网络维护服务项目服务清单

（以下无正文）

甲方：　　（盖章）

法定代表人或

授权代表（签字）：

签订日期：2025年5月30日

地址：

联系人：

电话：

传真：

开户银行：

银行账号：

乙方：　　（盖章）

法定代表人或

授权代表（签字）：

签订日期：2025年5月29日

地址：陕西省西咸新区沣西新城统一路中国联通西安数据中心办公楼102室

联系人：李莎

电话：15619133889

传真：

开户银行：中国工商银行西安高新区枫林绿洲支行

银行账号：3700028719020013049

附件 1：渭南市政务服务大厅硬件保障及网络维护服务项目服务清单

序号	项目分类	名称	模块功能	服务要求（服务标准）
1	网络巡检服务	防火墙系统巡检	规则审查：检查防火墙规则是否符合最新的安全标准，避免不必要的端口开放。 日志分析：分析防火墙日志，识别潜在的安全威胁，如恶意入侵尝试、异常流量等。 漏洞扫描：对防火墙设备进行定期漏洞扫描，确保没有已知的漏洞存在。 策略更新：根据网络环境的变化，及时更新防火墙策略，确保网络安全。性能评估： 检查防火墙设备的性能，确保其能承载当前的流量负载，并对可能的性能瓶颈进行优化。 报告与建议： 提供定期报告，总结防火墙巡检结果，并提出改进建议。	配合相关部门进行大厅防火墙系统巡检
2		路由器配置巡检	配置审查与对比： 定期获取路由器的当前配置，并与预设的安全标准或历史配置进行对比。 自动识别配置中的异常或潜在风险（如默认密码、未授权端口开启等）。 漏洞扫描与安全检测： 检查路由器是否存在已知的漏洞（例如未打补丁的固件、弱密码设置等）。 自动检测配置中可能导致安全隐患的部分（如路由器的访问控制列表 ACL 配置不当）。 配置备份与恢复： 定期备份路由器的配置，以防止配置丢失或错误更改。 提供简单的恢复机制，支持在出现配置错误时快速恢复到安全的先前版本。 性能监控： 监控路由器的性能指标，包括流量负载、CPU 利用率、内存使用情况等，确保设备处于健康状态。 提供流量分析报告，以帮助网络管理员优化路由器的配置。 日志分析与审计： 自动分析路由器的日志文件，检测异常访问、未授权操作或其他潜在的安全事件。 生成详细的审计报告，支持合规性检查和问题追溯。 自动化合规检查： 根据行业最佳实践或企业的网络安全政策，自动化检查配置项的合规性。 提供合规性报告，帮助网络管理员确保所有路由器配置符合规定的安全标准和合规要求。 多设备集中管理： 支持多设备集中管理，适用于大型网络或多个分支机构。 通过统一界面查看所有设备的配置状态、性能指标以及安全日志。 通知与警报系统： 配置巡检软件可在发现潜在问题时发送警报，例如配置项不符、安全漏洞或设备性能异常。	解决相关故障，建立巡检台账。

			支持与企业内部的监控系统或报警系统集成，实时通知相关人员进行处理。	
3		交换机配置巡检	自动检测和审查交换机的配置文件，发现可能的配置错误、冗余项或不符合最佳实践的设置。 通过与预设的安全模板和标准进行对比，确保配置的规范性。 检测交换机是否存在安全漏洞，包括不安全的访问控制（如开启了不必要的端口）、弱密码配置、过时的固件版本等。 提供建议来提升安全性，如强制使用 SSH 而不是 Telnet、禁用未使用的 VLAN 等。 持续监控交换机的 CPU、内存和端口负载，及时发现性能瓶颈或异常流量。 提供端口级流量分析报告，帮助管理员发现潜在的带宽问题或网络拥塞。 自动收集交换机的日志并进行实时分析，检测可能的安全事件、配置变更或硬件故障。 支持审计报告生成功能，用于内部合规性检查或问题追溯。 软件能够实时监控交换机状态，在设备出现故障或异常时自动触发报警，并提供修复建议。 支持配置错误自动修复，如恢复默认配置、重启交换机等操作。 定期备份交换机配置文件，避免由于配置丢失或意外更改造成网络故障。 提供简便的恢复功能，确保配置回滚快速且准确。 适合大规模网络环境，支持集中管理多个交换机设备。通过统一的平台查看配置差异、性能指标和安全警报，简化设备管理。 提供自动化报告生成功能，包括配置检查报告、性能分析报告和安全漏洞报告。 配置化的告警机制可通过邮件、短信等多种方式通知管理员，确保问题及时处理。	整理机柜线路，张贴线路标识，建立巡检台账。
4		公网链接状况巡检	实时公网链路状态监控 链路健康检查：定期检查公网链路的状态（如是否在线、响应时间等），及时发现链路中断或波动。 连接延迟监控：实时监控公网链路的延迟（Ping 值），并对高延迟情况进行标记，便于后续分析。 丢包监控：监测公网链路的丢包情况，通过丢包率判断链路是否存在不稳定的表现。 链路质量分析 带宽利用率分析：通过带宽监控，检查公网链路的带宽利用情况，识别是否存在带宽瓶颈或过度使用现象。 路由分析：对数据包传输的路由路径进行实时追踪，分析公网链接的路径稳定性，检测是否存在跳数过多或不合理的路由选择。 链路波动检测：检测链路的稳定性波动，自动识别链路异常波动（如周期性丢包、延迟抖动等），帮助管理员及时识别问题来源。 公网链路负载均衡检测 多链路负载监测：对于存在多条公网链路的网络环境，监控各链路的负载状况，确保流量均衡分布，避免单一链路过载。 负载优化建议：根据链路负载情况，提供流量优化建议或自动调节策略，确保网络负载均衡和链路高效利用。	绘制大厅网络拓扑图。对网络线路进行规整，移除废弃网线。汇总信息化设备 IP、MAC 地址，解决相关故障，建立巡检台账。

			自动化故障检测与报警 故障检测：通过定时探测公网链路，自动检测链路是否断开或出现故障，及时生成故障报告。 告警系统：在检测到链路故障、延迟超标或丢包过高等问题时，实时向管理员发送报警通知，支持邮件、短信或企业 IM 系统通知。 历史数据查询与报告生成 历史状态查询：支持查看公网链路的历史状态数据，方便管理员分析长期趋势和链路健康状况。 报告生成：根据链路状态、带宽使用、延迟和丢包数据，自动生成周期性的报告，帮助管理层了解链路性能、诊断问题及优化建议。 多链路环境支持 多 ISP 链路监控：对于使用多个 ISP（互联网服务提供商）链路的企业环境，支持同时监控多个公网链路的状态。 自动切换监控：在发现主链路出现故障时，自动切换到备用链路并进行监控，确保互联网连接的持续性。 可视化管理界面 图形化展示：提供图形化的实时监控界面，展示公网链路的状态、带宽利用率、延迟、丢包等关键指标，帮助管理员直观了解链路健康状况。 自定义视图：允许管理员根据需求自定义监控面板，选择显示特定链路的状态信息、性能数据或告警。 智能优化与建议 链路优化建议：基于实时数据和历史数据，系统会提供链路优化建议，例如调整链路负载分配、优化路由路径等。 自动修复建议：当检测到问题链路时，自动给出修复建议，例如切换链路、增加带宽或调整路由策略。	
5		电子监察系统及设备配置巡检	设备配置健康检查 设备状态监测：实时监控安防设备的运行状态，检查设备是否处于正常工作状态，及时识别掉线或故障设备。 配置文件审核：对每个安防设备的配置文件进行检查，确保设置符合企业或安全标准，例如摄像头的分辨率、录像存储路径、报警阈值等。 安全性检查 密码与认证审核：检查安防设备是否采用默认密码或弱密码，确保设备配置了强密码和必要的认证措施。 网络安全性检测：检测设备是否存在安全漏洞，如是否启用了不安全的协议（如 Telnet、FTP 等），是否有开放的管理端口等。 防篡改设置检查：检查安防设备是否启用了防篡改设置，防止设备配置被恶意修改。 设备性能监控 存储空间监控：定期监控录像存储设备（如 NVR、DVR）的存储空间使用情况，确保设备有足	解决相关故障，建立巡检台账。

			够的空间存储视频数据，并在存储空间不足时提前提醒。 带宽与负载监控：检查视频监控系统的带宽使用情况，分析网络负载，确保系统的视频流能够正常传输，避免因带宽不足导致视频延迟或卡顿。 设备兼容性检测 协议兼容性检查：检查安防设备之间的协议兼容性，确保各设备之间能够正确通信和协作。 版本检查与更新：确保设备使用的固件或软件版本是最新的，及时检测并提醒管理员进行更新，以解决已知的漏洞或性能问题。 故障诊断与告警 实时故障检测：通过主动巡检，自动发现安防设备的故障或异常状态（如设备离线、配置错误、存储不足等），并生成故障报告。 告警系统：一旦发现设备故障或安全问题，系统会立即通过邮件、短信、应用通知等方式向管理员发送告警，确保问题能够及时响应并解决。	
6		电子监察系统及设备网络巡检	网络连通性监测 实时监测安防设备的网络连接状态，检查设备是否在线、是否能正常与网络交换机、服务器等设备通讯。 带宽与延迟分析 定期检测设备的网络带宽使用情况及连接延迟，确保网络负载在正常范围内，避免因带宽不足或延迟过高影响设备性能。 丢包与故障检测 检测安防设备在网络传输过程中是否发生丢包或数据丢失，及时告警以防网络故障。 自动化告警与通知 一旦发现设备脱网、延迟异常或丢包等问题，系统会自动发出告警，通知管理员进行及时处理。 历史数据查询与报告生成 提供网络连接历史数据查看与分析，生成详细的报告，帮助管理员评估设备的网络稳定性。	解决相关故障，建立巡检台账。
7	信息系统巡检服务	内网设备信息巡检	设备状态监测 实时监控内网设备的在线状态，及时发现设备故障、离线或异常情况。 配置检查与合规性审计 自动检查设备配置是否符合预设标准，如安全设置、固件版本、IP 地址分配等。 性能监控 检查设备的 CPU、内存、硬盘使用情况及网络流量，避免因资源过载影响设备性能。 故障诊断与告警 对设备故障进行自动诊断，并生成实时告警，确保问题得到及时响应和解决。 报告生成与历史查询 自动生成设备巡检报告，支持查看历史巡检记录，帮助管理员进行设备维护和优化。	解决网络故障，建立相关巡检台账。
8		数据库巡检	数据库健康检查 实时监测数据库的运行状态，检查数据库是否正常响应查询、是否有异常崩溃或挂起等问题。	配合相关部门进行进行数据库相关设备巡

			性能监控 监控数据库的查询响应时间、内存和 CPU 使用情况，确保性能不受影响。 备份与恢复检查 检查数据库备份是否成功、是否按计划进行，确保数据在发生故障时可恢复。 安全性审计 检查数据库的访问权限、密码强度等安全配置，确保数据库不会受到未经授权的访问。 故障诊断与告警 自动诊断数据库故障，生成告警并及时通知管理员进行处理。 报告生成与历史查询 自动生成巡检报告，提供历史数据查询，帮助管理员进行分析和决策。	检
9		终端设备软件系统巡检	系统健康检查 实时监控各设备软件系统的运行状态，检查系统是否有异常进程、崩溃、死锁等问题。 资源使用检查 监控 CPU、内存、磁盘空间和网络带宽的使用情况，确保资源分配合理，避免系统过载。 服务状态检查 自动检查系统中关键服务（如 Apache、MySQL、SSH 等）是否正常运行，及时发现服务故障或异常。 日志分析与审计 自动分析系统日志文件（如/var/log 目录下的日志），检查错误、警告及潜在的安全问题，帮助及时发现故障。 安全性检查 检查系统的安全配置，包括 SSH 安全设置、账户权限、开放端口、防火墙状态等，确保系统免受未授权访问和攻击。 更新与补丁管理 自动检查系统是否有可用的安全更新和补丁，并提醒管理员及时安装，以保持系统安全性。 故障诊断与告警 发现系统异常或故障时，自动诊断并生成告警，通知管理员进行及时处理。 报告生成与历史查询 自动生成巡检报告，支持查看历史巡检记录，帮助管理员做出基于数据的维护决策。 自动生成巡检报告，支持查看历史巡检记录，帮助管理员进行系统维护和优化。	采用软件，实时监测实时监测操作系统的运行状态，检查系统是否有错误日志、崩溃或异常进程等问题。 定期查杀病毒和升级补丁策略，解决相关故障，建立相关巡检台账。
10	网络应急服务	网络应急服务	故障检测与定位 通过实时监控和诊断工具，迅速检测到网络中断或性能下降等问题，并定位问题根源。 网络攻击应急响应 针对 DDoS 攻击、病毒入侵、木马、恶意软件等网络安全威胁，提供迅速的应急响应，包括流量清洗、入侵检测与防护、隔离受感染主机等措施。 灾难恢复与备份 针对网络中断或数据丢失，提供灾难恢复方案和备份数据恢复服务，确保系统的持续性和数	邀请网络安全相关专家，组织一次网络安全培训活动。

			据的完整性。 性能调优与修复 当出现网络性能瓶颈（如延迟高、带宽不足、丢包等问题）时，迅速评估并修复，优化网络结构和配置。 紧急技术支持与远程协助 提供 24/7 的技术支持服务，在紧急情况下，技术团队可远程或现场进行问题排查和解决。	
11	网络安全攻防演练服务	网络安全检测及网络安全防攻演练	红蓝对抗演练 红队（攻击方）：模拟黑客攻击，采用各种技术手段（如社交工程、漏洞利用、恶意软件等）发起攻击，目标是突破组织的网络防线。 蓝队（防守方）：负责防御和应对红队的攻击，采取措施（如入侵检测、漏洞修复、访问控制等）确保网络安全。 渗透测试 模拟黑客通过网络漏洞、配置错误或弱密码等方式，尝试渗透到组织的内部系统和网络，测试防护措施的有效性。 漏洞扫描与修复 在演练过程中，自动化工具会扫描系统和应用程序中的安全漏洞，蓝队需识别并修复这些漏洞，避免真实攻击的发生。 入侵检测与响应 测试现有的入侵检测系统（IDS/IPS）、日志分析工具和防火墙规则的有效性，评估组织在发现攻击后能否迅速做出响应。 安全事件分析与报告 演练结束后，红队和蓝队会共同进行事件回顾，分析攻击的过程、防御措施的效果，以及改进的空间，生成详细的安全演练报告。 应急响应演练 测试组织的应急响应流程，确保在网络攻击发生时，相关部门能迅速协调应对，降低损失。 安全意识培训 演练过程中还可以进行安全意识培训，提升员工在面对钓鱼攻击、恶意链接等社交工程攻击时的防范能力。 组织模拟场景化的网络攻防（包括但不限于 DDoS 攻击（分布式拒绝服务攻击）、 钓鱼攻击、SQL 注入、恶意软件（勒索软件、挖矿木马等）、中间人攻击（MITM）、零日攻击、社会工程学与密码攻击、供应链攻击、物联网与边缘设备攻击、高级持续性威胁（APT）	开展一次网络安全应急演练。
12	舆论监测服务	舆论监测服务	实时舆情监测 通过智能化工具和技术，持续扫描互联网、社交平台、新闻网站、论坛等多个信息来源，实时收集与目标关键词、品牌、事件相关的舆论动态。 舆情热点识别	第一时间发现网络舆情，并处理解决。

			自动识别当前舆情的热点和趋势，及时捕捉突发事件、公众关注的热点话题，帮助企业或组织快速了解舆论焦点。 情绪分析与趋势预测 通过自然语言处理（NLP）和情感分析技术，分析公众的情绪倾向（如正面、负面或中性），并预测舆情的未来发展趋势。 舆情报告生成 定期或按需生成舆情监测报告，提供舆论的综合分析、情感态度、趋势变化以及潜在的风险点，帮助决策者了解公众意见。 危机预警与响应 根据舆情的发展动态，提供危机预警和响应建议。通过监控舆情的变化，提前发现潜在的危机，并提供应对策略，避免舆情失控。 舆论引导与干预 对于负面舆情，提供舆论引导建议，帮助企业或个人制定有效的公关策略，通过发布澄清声明、参与舆论互动等方式，积极干预并引导舆论走向。 竞品与行业对比分析 监测和分析竞品的舆情状况，了解竞争对手的舆论趋势和公众反馈，帮助企业在市场中制定更有利的品牌策略。	
13	设施设备服务	硬件保障服务	1.维保设备清单 电子设备：电脑、LED 抬头屏、LED 大屏、打印机、高拍仪、呼叫器、网络交换机、人证对比机、抽号机、电视机、网络分配器、收发器、网络录音盒等电子设备； 安防设备：安防摄像头、监控大屏、拼接器、安防交换机、安防平台、存储服务器、核心路由器等； 办公家具：沙发、桌子、椅子、门把手、门锁、隔离桩、资料架、资料柜、办公区格挡、冬夏季门帘等。	对电子设备进行每班前班后开关及巡查，及时维修故障设备，并建立维修记录。 确保沙发、桌子、椅子使用过程安全无故障。门把手、门锁.隔离桩、资料架、资料柜、办公区格挡、冬夏季门帘等正常使用，无破损及损坏现象。