2026年西安市住建局城建档案馆
机房硬件新运维项目

服务合同

甲　方：西安市城建档案馆

乙　方：开利科技股份有限公司

2026年11月

甲方：西安市城建档案馆

地址：西安市欧亚六路 1 号

法定代表人：张春峰

联系方式：029-89623001

乙方：开利科技股份有限公司

地址：云南省昆明市盘龙区云南映象城市公园广场 1 幢 12 层 1207 号

法定代表人：齐转风

联系方式：0871-63319009

按照政府采购程序组织竞争性磋商，最终确定乙方为 2026 年西安市住建局城建档案馆机房硬件新运维项目成交供应商。依据《中华人民共和国民法典》以及竞争性磋商文件、成交通知书，经甲、乙双方协商，达成如下合同条款。

一、合同标的物内容及数量（以响应文件正本和澄清表〈函〉为准，详见附件）

项目名称	服务内容	合计	服务期
2026 年西安市住建局城建档案馆机房硬件新运维项目	对机房核心服务器、存储、交换机、网络设备等进行常规维 护和故障维修，对服务器运行必须的操作系统、数据库软件和保障网络安全的杀毒软件进行升级维护；对机房的空调、新风系统、UPS 等环境设备硬件进行日常维护和故障维修；确保数据库、存储、网络、安全等相关设备正常、平稳、安全、可靠运行。对各维保设备进行每日例行巡检及相关故障处理工作。保障西安市城建档案馆信息化基础设备、网络及安全产品等正常运转，保证档案管理	339000.00	合同签订之日起 1 年

	系统持续稳定运行。		
合计（大写）	人民币叁拾叁万玖仟元整		

二、服务条件

1、服务地点：西安市城建档案馆

2、服务期限：自合同签订之日起1年。

三、合同价款

1、合同总价款为人民币（大写）叁拾叁万玖仟元整（￥339000.00 元）。

2、合同总价包括：维保费和其它全部费用。

3、合同总价一次性包死，不受市场价格变化因素的影响。

四、款项结算

1、合同签订之日起10个工作日内，乙方持中标通知书、合同、当期付款金额的普通增值税发票（信息技术服务，税率6%，下同），与甲方结算合同总价款的30%，即人民币（大写）（壹拾万壹仟柒佰元整）。

2、乙方正常提供维保服务，达到服务标准且经甲方书面确认后，于2027年尾款资金下达后，乙方持当期付款金额的增值税普通发票，与甲方结算合同总价款的50%，即人民币（大写）（壹拾陆万玖仟伍佰元整）。

3、服务期满并经甲方验收合格后，填写项目验收意见书（一式三份），验收通过之日起一个月内，乙方持项目验收意见书、当期付款金额的增值税普通发票，与甲方结算合同当期应付款。当期付款金

额=合同总价款的20%，即人民币（大写）（陆万柒仟捌佰元整）。

4、上述正常提供维保服务是指由甲方指定的项目负责人对乙方正常服务状态进行签字确认。

5、支付方式：银行转账。甲方通过转账方式将应付乙方款项付至乙方指定下列账户：

户　名：开利科技股份有限公司

开户行：中国工商银行股份有限公司昆明北京路支行

账　号：2502014009200048329

五、维保服务质量标准

1、服务方案和方式科学、可行，全面满足各项服务要求。设备及系统维护符合国家有关服务规范要求，确保甲方设备及系统达到最佳运行状态。

2、有专门的维保小组，分工明确（应有具体成员名单，包括姓名、所在公司、职务、职称、工作职责、联系方式等）。乙方必须提供投标文件中承诺的技术服务团队，在甲方指定的地点和环境中，驻现场进行维保服务工作，该团队在服务期间未经甲方书面同意不得从事其他任何工作。

3、有各类突发事件的应急预案，且具有可操作性，并提交采购人审核通过。

4、驻场服务人员、维保服务人员能满足要求并完成服务任务。乙方维保服务过程中使用的软件系统，若发生侵权而产生的一切后果，由乙方负责，甲方保留索赔权力。

5、乙方承诺，因乙方原因造成的服务期内本项目涉及的所有人员伤亡、财产损失等安全责任均由乙方承担。

六、双方的权利和义务

（一）甲方的权利和义务

1、为了保证甲方系统安全和保密要求，在项目服务期间，甲方提供服务地点和环境。

2、在乙方进行现场升级与维护时，甲方应按乙方的要求提供相应的软件、硬件及网络环境，保证项目的顺利实施。

3、在甲方安全规定允许的前提下，为乙方的人员进入升级维护现场提供方便。

4、甲方及时将本合同下维护范围内出现的故障情况通知乙方，乙方在指定期限内响应并作出故障处理方案。乙方应负责做好故障有关资料的记录工作。

5、如不能证明甲方为故意，甲方对乙方工作人员的人身及财产的安全不负任何责任。因乙方或其工作人员的行为造成第三人损害的，与甲方无关，由乙方承担全部责任。

6、甲方有权对乙方工程师的工作态度、技术水平进行监督和评判并提出相应的要求，乙方也会由独立的服务质量监督人员对甲方予以不定期的回访。

7、甲方负责提供故障发生前后相关的系统或设备资料、数据和原始记录。

（二）乙方的权利和义务

1、乙方确保提供维护服务的系统能够稳定安全的运行，满足招标/投标文件要求。

2、按照合同要求在规定时间内提供专业化技术人员在甲方现场驻守，确保系统及设备正常运行。

3、乙方为甲方提供定期巡检，做好预防性维护。

4、乙方进入甲方机房，必须经甲方同意后，并由甲方或项目监理人员陪同，同时遵守机房的各种规定。

5、乙方在甲方机房操作期间必须由甲方或项目监理人员进行现场监督，所进行的操作必须经过甲方同意；工作结束后，需经甲乙双方现场人员检查系统，书面确认操作内容和操作达到目的，且系统及设备运行正常后方可离开现场。

6、乙方保证在甲方现场的工作人员严格按照甲方现场管理要求和工作纪律行事。

7、乙方应按甲方要求如期向甲方交付相关文档，如定期的巡检报告、服务报告、现场服务单等。

8、乙方在服务过程中发现非本合同服务范围内的相关问题导致系统故障，应及时向甲方汇报，在获得甲方书面的许可和费用确认后，双方签订补充协议，明确该故障问题的维护内容、费用标准及期限等事项。乙方应向甲方提供不低于本合同约定服务范围内设备及软件的运行维护服务。

9、乙方提供维保服务期间，应当保证甲方设备、网络、应用系统及数据的安全，并对甲方的所有相关数据及技术信息进行保密，不得外泄。

10、乙方应当按照招标文件要求硬件设备的种类、品牌、型号、套数准备相应的备品备件，保证备品备件是正品、全新、未拆封的，并将备件置于甲方安排的场所，以便出现故障时，尽快修复，更换的备件应交由甲方处理。

11、因硬件维保导致备品备件不足的，乙方应当按照招标文件约定 2 周内补足备品备件，该费用已包含在合同总价款内，甲方不再

另行支付。

12、乙方应在故障发生后 2 小时内完成修复，保证软、硬件正常运行。如遇不可抗力，双方可另行协商前述时间。

13、乙方承诺并保证，本合同服务期满，若甲方需要，乙方可延长服务期至甲方完成下一年度机房硬件运维项目采购工作，共同保障甲方系统的平稳运行。

七、保密

1、乙方应遵守国家有关保密的法律法规和行业规定，并对甲方及关联方提供的资料负有保密义务。乙方驻场人员须签订保密承诺书。未经甲方书面同意，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披露、提供给其他单位和个人，或用作本合同外用途。如发生以上情况，甲方有权索赔。

2、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。

3、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。

4、保密期限：长期。

5、保密费用已包含本合同总价款内，甲方不再另行向乙方支付保密费用。

八、知识产权及承诺

1、供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其他

知识产权而引起的法律和经济纠纷，如存在前述情形，由供应商承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

2、供应商将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

3、如采用供应商所不拥有的知识产权，则在报价中必须包括合法使用该知识产权的相关费用。

4、构成本磋商文件的各组成部分，未经采购人书面同意，供应商不得擅自复印或用于非本磋商项目所需的其他目的。

九、验收

1、服务期满后，甲方根据采购文件、响应文件及相关文件资料，进行考核验收，确认服务标准和服务方式是否达到采购要求。验收资料包括但不限于服务方案、项目月报、巡检记录单、应急演练方案及报告、培训记录、备品备件更换材料、运维总结报告等资料。

2、甲方组织乙方，必要时请有关专家进行考核验收，验收合格后，填写项目履约验收意见书（一式三份）作为对维保服务的最终认可，乙方未在甲方指定的时间参与验收的，视为认可甲方的验收结果。

3、乙方按照甲方要求的期限向甲方提供服务过程中的所有资料，须整理成册，以便甲方日后管理和维护。

4、验收依据

（1）采购文件、响应文件、澄清表（函）；

（2）本合同及附件文本；

（3）合同签订时国家及行业现行的标准和技术规范，合同履行

过程中相关标准和规范发生变化的，按照最新的标准及规范执行。

十、违约责任

（一）乙方未按合同要求提供产品、服务或不能满足合同要求，甲方应当将乙方违约的情况以及拟采取的措施以书面形式报政府采购监管部门，根据政府采购监管部门的处理意见，甲方有权依据《中华人民共和国民法典》有关条款及合同约定终止合同，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。

（二）出现下列情形之一的，甲方有权要求中标供应商按照合同总价款的20%承担违约责任，如造成甲方的损失大于违约金的，还应承担赔偿责任：

1、乙方逾期不实施项目工作计划，但逾期不足10天的；

2、乙方未按照响应文件配置设施人员的；

3、乙方没有按照合同约定或甲方要求时间完成项目的；

4、乙方完成并向甲方提交的项目成果未能通过验收的；

5、乙方或乙方的工作人员违反保密义务的；

6、乙方提供的技术侵犯他人合法权益的；

7、乙方未能在合同约定的时间内达到现场处理故障，次数超过3次的；

8、违反甲方相关管理规定，经甲方提出整改要求且拒不整改的；

9、乙方未按采购文件要求及时补充备品备件的；

10、乙方在服务过程中未发现问题或未按照合同及附件要求进行服务，直接或间接造成系统或设备故障的；

11、乙方违反的合同义务的其他行为的。

（三）甲方逾期付款的，成交供应商有权要求甲方以当期应付未付款项为基数，每逾期一日按照日万分之五支付违约金，但不得超过当期应付未付款项的10%。

（四）乙方出现下列情形之一的，甲方有权解除合同，乙方除应返还甲方已支付的全部价款外，还应按照合同总金额30%的向甲方承担违约责任，如造成甲方的损失大于违约金的，还应承担赔偿责任：

1、未经甲方书面同意，擅自将合同项下全部或部分义务转包或分包第三人的；

2、乙方提供的技术服务致使甲方设备、系统损坏的；

3、乙方未按相关条款及附件约定的时间或条件对软件进行修改、升级的，或进行修改、升级的软件经测试验收不合格，又未在甲方指定的时间内负责修改或测试的；

4、乙方提供的技术服务侵犯第三人权益的，且未能在甲方指定的时间内解决的；

5、乙方未按照投标文件配置设施人员或者未经甲方书面许可擅自变更人员或开发团队的，且未在甲方指定的时间内改正的；

6、乙方逾期不实施项目工作计划，且逾期超过 10 天；

7、违反甲方相关管理规定，经甲方提出整改要求且拒不整改，并造成具体的损害后果的；

8、乙方未按招标文件要求及时补充备品备件的，且甲方催告后，仍未补充备品备件的；

9、乙方在服务过程中未发现问题或未按照合同及附件要求进行服务，直接或间接造成系统或设备故障，且未及时采取必要措施或未及时报备的；

10、其他严重违反本合同约定的行为。

合同解除异议期为一个月，自收到解除通知之日起计算。

（五）因一方的违约行为导致受约方受损的，违约方除应承担相应的违约责任外，还应赔偿守约方的损失，包括但不限于诉讼费、律师费、差旅费、保函费、鉴定费以及因违约方的违约行为导致守约方先行赔付费用等。

十一、争议解决

若在本合同履行过程中发生争议，甲乙双方协商解决；协商不成的，任何一方均有权向甲方所在地人民法院提起诉讼。

十二、其他

1、出现不可抗力事件时，知情方应及时、充分地向对方以书面形式发通知，并告知对方该类事件对本合同可能产生的影响，并应当在合理期限内提供相关证明。由于以上所述不可抗力事件致使条款的部分或全部不能履行或延迟履行，则双方于彼此间不承担任何违约责任。

2、本合同未尽事宜，双方协商解决，并签订书面补充协议。

3、本合同一式伍份，经甲乙双方法定代表人/授权代表签字盖章后生效。甲方执肆份，乙方执壹份，具有同等法律效力。

（以下无正文）

甲方（盖章）：西安市城建档案馆

地址：西安市欧亚六路 1 号

法定代表人（签字）：

签订日期：2026 年 11 月 17 日

乙方（盖章）：开利科技股份有限公司

地址：云南省昆明市盘龙区云南映象城市公园广场 1 幢 12 层 1207 号

法定代表人（签字）：

签订日期：2026 年 11 月 17 日

附件：

参数性质	序号	技术参数与性能指标
	1	一、硬件运维 1、维护内容：提供产品支持、服务器、存储、数据库维护、空调、UPS 维护、网络维护、定期巡检等服务。 **1.1 产品技术支持服务** （1）提供 7*24 小时热线电话服务，随时解答我单位的问题，为我单位提供紧急支持。 （2）提供维修及换件服务：接到故障通知后，保证在 4 小时内恢复到系统原有正常运行状态。 （3）提供 1 人现场驻场服务。 （4）提供其它情况下的现场服务：如果我单位非工作时间遇到特殊或紧急情况，要求服务技术人员现场值班，须提供现场协助。 **1.2 服务器、存储、数据库维护** 1.2.1 核心设备硬件运维 （1）提供对系统性能优化提供建议及支持服务； （2）提供对系统安全、网络配置提供建议及支持服务； （3）提供现场进行疑难问题解决及故障处理服务； （4）提供现场进行性能优化服务； （5）提供现场进行系统配置服务； 1.2.2 数据库维护 （1）提供数据库备份与恢复服务： （2）提供对数据库性能优化提供建议及支持服务 （3）提供对数据库安全、参数配置提供建议及支持服务 （4）提供现场进行数据库疑难问题解决及故障处理服务 （5）提供现场进行数据库性能优化服务 （6）提供现场进行数据库配置服务 1.2.3 存储维护 （1）提供存储性能优化相关建议及技术支持 （2）提供存储现场性能调优及优化实施服务 （3）提供存储现场配置部署及调试服务 1.2.4 操作系统维护及补丁升级服务 （1）对操作系统的日常运行维护服务，包含日常维护、管理、配置调整、优化及故障处理等。 （2）提供补丁安装支持服务； （3）提供安装完成后对系统进行测试和备份服务。 1.2.5 光纤交换机维护服务 （1）提供光纤交换机性能优化建议及 7×24 小时远程技术支持。 （2）提供光纤交换机现场性能调优及优化实施服务。 （3）提供光纤交换机现场配置部署、调试及设备联调服务

		1.2.6 世安 T5-A 中间机维护服务 （1）提供世安中间机配置部署、维护、调试服务 （2）提供世安中间机故障维修服务 **1.3 空调、UPS 维护** 1.3.1 空调系统维护服务 外观检查： （1）提供检查空调面板显示是否正常服务； （2）提供检查空调面板显示值与测量值是否一致（在允许的范围内）服务； （3）提供各种操作按键是否灵活可靠服务。 系统检查： （1）提供检查主要部件及易损件（压缩机、加湿罐、风机、干燥器、过滤网等）的工作状态服务； （2）提供机内除尘，表面清洁以及过滤网定期更换服务； （3）提供清洗室外冷凝器服务。 1.3.2 UPS 不间断电源维护服务 外观检测： （1）提供检查机器面板显示是否正常服务； （2）提供检查面板显示值与测量值是否一致（在允许的范围内）服务； （3）提供各种操作按键是否灵活可靠服务； （4）提供用电环境检查服务。 系统检查： （1）提供检查 UPS 输入、输出空开温度及运行情况服务； （2）提供测量地线阻值、零地电压是否符合标准服务； （3）提供测试市电和电池相互转换是否正常，手动旁路是否可靠服务； （4）提供对 UPS 进行放电测试服务； （5）提供检查电解电容器是否有漏液、冒顶和膨胀现象发生服务； （6）提供检查变压器线圈、连接器件、扼流圈等是否有过热、色变、分层脱落现象，并确认每个连接线口牢固服务； （7）提供检查电缆是否有老化龟裂、掉渣、划伤和破裂服务； （8）提供检查各处断路器和模块服务； （9）提供蓄电池外观是否有氧化腐蚀、漏液现象服务； （10）提供蓄电池动态逐块测试电池的浮充电压服务； （11）提供用测试工具在线测试电池的放电电流或用电池内阻测试仪在线测试电池的内阻服务； （12）提供在条件允许的情况下，逐块测试电池的放电电压，判断电池的好坏，以防市电中断后负载断电服务； （13）提供检查接线端子：检查电池及 UPS 输入、输出端子是否牢靠服务； （14）提供机内除尘：每年视机内积尘程度提供 1 次机内除尘服务。 **1.4 网络维护** 1.4.1 网络、安全设备维护服务 ①对使用过程遇到的疑难问题进行技术支持；

②对设备性能优化提供建议及技术支持；

③对设备配置提供建议及技术支持；

④现场进行故障问题解决；

⑤现场进行性能优化；

⑥现场进行系统参数配置；

1.4.2 网络、安全设备软件升级服务

①必须提供网络、安全设备操作系统必要的升级与性能调优；

②网络、安全设备操作系统软件的补丁安装；

③提供故障诊断和修复；

④安全设备特征库定时升级服务。

1.4.3 性能诊断与调试

对采购人网络、安全硬件系统情况进行性能诊断，根据结果调整系统参数，使系统始终在最佳状态下运行。对可能出现的问题提供科学预测，并采用必要的预防和补救措施，防患于未然。具体如下：

①检查网络设备系统硬件使用情况；

②检查网络安全设备策略；

③检查网络安全设备特征库升级情况。

1.5 定期巡检维护

1.5.1 每日定期2次巡检服务，巡检内容包括但不限于：

（1）机房基础环境（空调、UPS、新风机）运行状态检查

（2）各硬件设备健康状态灯检查

（3）各服务器资源使用率检查

（4）数据库运行状态、性能指标等检查

2、维护要求及目标

2.1 确保系统安全、稳定、高效运行。对于维保范围内系统出现的任何故障，当故障发生后保证在2小时（RTO）内恢复到系统原有正常运行状态。

2.2 因设备软硬件故障引起的操作系统、数据库等软件出现问题，应及时恢复至故障前状态。

2.3 对于系统故障处理应有详细的报告记录，包含故障原因、响应时间、解决方案以及合理建议等。

2.4 提供全年 5*8h 现场服务能力，在服务期内，需提供驻场服务，驻场技术人员除每日进行2次机房基础环境（空调、UPS、新风机）、服务器、存储等所有维保设备的日常巡检，故障处理外，还需处理我单位机房相关的其它事务，包括但不限于：处理客户终端电脑、打印机等办公设备的问题。

3、交付成果

序号	主要服务内容	交付频次	交付物
1	每天2次机房基础环境、设备、数据库、操作系统相关巡检等	1册/月	《日常巡检册》
2	每月月初编写上月整体运行评估分析报告，主要内容包括系统运行信息、设备运行状态，服务事件汇总、容量趋势分析，数据库性能分析、	1册/月	《整体运行评估分析报告》

	网络设备性能分析等	
3	每年进行一次应急演练，演练相关数据库、存储、网络、硬件设备双活功能，多链路可靠性等	1次/年	《应急演练方案》和《应急演练总结》
4	组织厂家或维护人员不定期进行空调、UPS、数据库、网络、网络安全等方面日常维护及管理的培训，每次培训时长不少于2小时，每年不少1次	1次/年	《培训记录表》及培训资料

二、安全运维

1、维护内容

1.1 防火墙安全服务

1.1.1 防火墙基础安全配置服务

（1）核心目标：确保防火墙初始配置合规、基础防护生效，规避默认配置带来的安全风险，贴合用户网络架构实际需求。

（2）设备初始化与合规配置：检查防火墙现有配置，清理默认账号、弱口令，修改管理员登录密码（设置复杂度要求），关闭不必要的默认端口、服务及管理协议（如Telnet），启用SSH加密登录并限制登录IP，确保管理员访问安全。

（3）网络接口与区域划分：根据用户网络架构，合理划分安全区域（如信任区、非信任区、DMZ区），配置各接口IP地址、路由策略，确保区域间隔离有效，仅开放必要的接口通信，杜绝跨区域违规访问。

（4）基础防护策略配置：配置默认拒绝策略（除明确允许外，拒绝所有进出流量），梳理用户业务所需的端口、协议，精准配置访问控制策略（ACL），明确源IP、目的IP、端口、协议的匹配规则，避免策略冗余、过宽导致的安全漏洞。

（5）日志与审计配置：启用防火墙日志功能，配置日志存储路径（本地存储+定期导出备份），明确日志记录范围（访问控制、登录操作、设备异常、攻击事件等），确保日志可追溯、可审计，满足合规要求。

1.1.2 防火墙日常运维与巡检服务

（1）核心目标：保障防火墙稳定运行，及时发现设备异常、策略隐患，确保防护功能持续有效，降低设备故障及安全风险。

（2）定期巡检（每日1次）：检查防火墙运行状态，包括CPU、内存、磁盘使用率，接口连接状态，电源、风扇等硬件状态，排查设备硬件故障及性能瓶颈；检查日志运行情况，确保日志正常记录、无丢失。

（3）策略优化与清理（每月1次）：梳理现有访问控制策略，删除过期、冗余、无效策略，合并重复策略，优化策略优先级，确保策略精准、高效，减少策略冲突及安全隐患；检查策略是否符合用户业务最新需求，及时调整策略配置。

（4）设备固件与补丁更新（每季度1次，紧急补丁及时更新）：查询防火墙厂商官方补丁发布情况，评估补丁兼容性及安全性，在不影响业务运行的时段（如夜间）更新固件及安全补丁，修复设备自身漏洞，提升设备防护能力。

（5）配置备份与恢复：每周备份防火墙完整配置文件，存储在安全的本地及异地位置，明确备份命名规则（含日期、设备型号）；每半年开展1次配置恢复测试，确保备份文件有效，可在设备故障时快速恢复配置，减少业务中断时间。

1.1.3 防火墙安全防护与监测服务

（1）核心目标：依托防火墙自身防护能力，抵御常见网络攻击，实时监测网络

		流量异常，及时发现并处置安全事件。 （2）攻击防护配置与运维：启用防火墙内置攻击防护功能，包括 SYN Flood、UDP Flood、ICMP Flood 等 DDoS 攻击防护，配置合理的防护阈值；启用端口扫描、暴力破解防护，限制单 IP 尝试登录次数，抵御恶意扫描及暴力攻击。 （3）实时流量监测与分析：每日监测防火墙进出流量，重点关注异常流量（如流量突增、异常 IP 访问、违规端口通信），分析流量来源及目的，判断是否存在攻击行为或违规访问，及时上报异常情况并处置。 （4）安全事件排查与处置：针对防火墙日志中记录的安全事件（如攻击告警、违规访问、策略命中异常），及时排查事件原因，区分误报与真实攻击，采取针对性处置措施（如调整策略、封禁异常 IP、阻断攻击流量），形成事件处置报告。 （5）访问行为审计：定期审计防火墙访问控制策略执行情况，检查是否存在违规访问行为（如未授权 IP 访问核心业务、违规端口开放），排查策略漏洞，提出优化建议，确保网络访问合规。 **1.1.4 应急处置与故障排查服务** （1）核心目标：快速响应防火墙设备故障及安全应急事件，最大限度降低事件对用户业务的影响，确保网络边界安全可控。 （2）应急响应（7×24 小时）：接到防火墙相关应急需求（如设备宕机、网络中断、大规模攻击、策略异常），立即响应，远程或现场排查问题，优先恢复业务正常运行，再深入排查根本原因。 （3）设备故障排查：针对防火墙硬件故障（如电源故障、接口故障）、软件故障（如固件异常、配置错误），快速定位故障点，采取修复、重启、配置回滚等措施，确保设备快速恢复正常运行；无法现场修复的，协助对接厂商进行设备维修或更换。 （4）安全事件应急处置：发生网络攻击、违规访问等安全事件时，依托防火墙日志及防护功能，定位攻击源、攻击方式，采取阻断攻击、封禁 IP、调整策略等措施，遏制事件扩散；事件处置完成后，分析事件原因，优化防护策略，形成应急处置总结报告，避免同类事件再次发生。 **1.2 服务器安全服务** **1.2.1 服务器基础安全配置服务** （1）核心目标：确保服务器初始配置合规、基础防护生效，规避默认配置带来的安全风险，贴合用户业务系统实际部署需求。 （2）系统初始化与合规加固：检查服务器现有系统配置，清理默认账号、冗余账户及弱口令，修改管理员登录密码（设置复杂度要求及定期更换规则），关闭不必要的默认端口、无用服务，禁用危险系统命令，启用账号登录审计，确保管理员访问安全可控。 （3）账户与权限精细化配置：根据用户业务岗位分工，合理分配服务器账户权限，遵循“最小权限原则”，杜绝超权限访问；设置账户锁定机制（多次登录失败锁定），清理过期账户、临时账户，定期核查账户权限合理性，防范权限滥用风险。 （4）基础安全基线配置：配置服务器防火墙（系统自带/第三方），精准放行业务所需端口、协议，默认拒绝所有未授权进出流量；开启系统安全防护功能（如 Windows 防火墙、Linux SELinux），关闭不必要的远程桌面、文件共享等风险

		功能，筑牢服务器基础安全防线。 （5）日志与审计配置：启用服务器系统日志、应用日志功能，配置日志存储路径（本地存储+异地备份），明确日志记录范围（登录操作、权限变更、系统异常、应用报错等），确保日志可追溯、可审计，满足合规要求。 **1.2.2 服务器日常运维与巡检服务** （1）核心目标：保障服务器稳定运行，及时发现系统异常、安全隐患，确保防护功能持续有效，降低设备故障及业务中断风险。 （2）定期巡检（每日 1 次）：检查服务器运行状态，包括 CPU、内存、磁盘使用率，进程运行情况，网络连接状态，电源、硬件温度等工况，排查设备硬件故障及性能瓶颈；检查日志运行情况，确保日志正常记录、无丢失、无异常告警。 （3）安全策略优化与清理（每月 1 次）：梳理服务器现有防火墙规则、权限配置，删除过期、冗余、无效规则及权限，合并重复配置，优化策略优先级，确保策略精准、高效；检查配置是否符合用户业务最新需求，及时调整安全配置。 （4）系统补丁与组件更新（每季度 1 次，紧急补丁及时更新）：查询服务器操作系统、应用组件官方补丁发布情况，评估补丁兼容性及安全性，在不影响业务运行的时段（如夜间）安装系统补丁、应用组件更新，修复系统及应用自身漏洞，提升服务器防护能力。 （5）配置与数据备份：每周备份服务器系统配置、核心业务数据，存储在安全的本地及异地位置，明确备份命名规则（含日期、服务器名称、备份类型）；每半年开展 1 次备份恢复测试，确保备份文件有效，可在服务器故障、数据丢失时快速恢复，减少业务中断时间。 **1.2.3 服务器安全防护与监测服务** （1）核心目标：依托服务器安全防护工具，抵御常见服务器攻击，实时监测系统异常行为，及时发现并处置安全事件。 （2）恶意攻击防护配置与运维：启用服务器防病毒、入侵检测/防御功能，定期更新病毒库、攻击特征库；防护勒索病毒、木马、蠕虫等恶意程序，拦截恶意代码注入、缓冲区溢出等攻击行为；配置文件完整性监控，及时发现并处置文件被篡改情况。 （3）系统与流量实时监测：每日监测服务器系统资源占用、进程运行、端口连接等状态，重点关注异常行为（如陌生进程、异常端口占用、CPU/内存突增）；监测服务器进出流量，排查异常连接、恶意访问，判断是否存在攻击行为或违规操作，及时上报异常情况并处置。 （4）安全事件排查与处置：针对服务器日志中记录的安全事件（如病毒告警、权限异常、文件篡改、攻击行为），及时排查事件原因，区分误报与真实攻击，采取针对性处置措施（如清除恶意程序、封禁异常 IP、恢复被篡改文件、调整安全策略），形成事件处置报告。 （5）访问行为审计：定期审计服务器登录行为、权限操作、文件访问等情况，检查是否存在违规访问、权限滥用、恶意操作等行为，排查安全漏洞，提出优化建议，确保服务器访问合规。 **1.2.4 应急处置与故障排查服务** （1）核心目标：快速响应服务器设备故障及安全应急事件，最大限度降低事件对用户业务的影响，确保服务器安全可控。 （2）应急响应（7×24 小时）：接到服务器相关应急需求（如服务器宕机、系

统崩溃、数据丢失、大规模攻击、病毒爆发），立即响应，远程或现场排查问题，优先恢复业务正常运行，再深入排查根本原因。

（3）设备与系统故障排查：针对服务器硬件故障（如电源故障、硬盘故障、主板故障）、系统故障（如系统崩溃、启动失败、配置错误），快速定位故障点，采取修复、重启、系统恢复、配置回滚等措施，确保服务器快速恢复正常运行；无法现场修复的，协助对接厂商进行设备维修或更换。

（4）安全事件应急处置：发生病毒感染、勒索攻击、数据泄露、恶意篡改等安全事件时，依托服务器安全工具及日志数据，定位攻击源、攻击方式，采取隔离感染文件、清除恶意程序、封禁攻击 IP、恢复备份数据等措施，遏制事件扩散；事件处置完成后，分析事件原因，优化防护策略，形成应急处置总结报告，避免同类事件再次发生。

2、维护要求及目标

（1）保障服务器稳定运行：通过常态化巡检、漏洞修复与安全加固，及时处置服务器系统漏洞、异常行为，最大限度减少安全事件导致的服务器宕机，确保核心服务器可用性达 99.9%以上。

（2）强化边界防护能力：优化防火墙策略，规范端口开放、访问控制规则，抵御外部扫描、恶意入侵、端口攻击等威胁，筑牢网络边界安全防线。

（3）守护服务器数据安全：建立服务器数据备份、防泄露机制，防范数据篡改、丢失、非法访问等风险，符合《网络安全法》《数据安全法》等基础合规要求。

（4）规范安全运维流程：针对防火墙与服务器，建立标准化的巡检、策略调整、漏洞管理、应急处置流程，明确运维责任，提升运维效率。

（5）提升应急响应能力：建立针对防火墙、服务器的安全事件应急响应机制，快速处置入侵攻击、服务器故障等事件，减少安全损失。

3、交付成果

序号	主要服务内容	交付频次	交付物
1	每天 2 次防火墙、服务器安全巡检	1 册/月	《日常巡检册》
2	每月开展 1 次服务器漏洞扫描，重点扫描操作系统漏洞、应用程序漏洞，对发现的漏洞按严重程度（高危、中危、低危）分级，明确修复优先级与时限	1 次/月	《漏洞扫描报告》
3	按照漏洞扫描报告中发现的漏洞，进行修复，输出漏洞处理报告	按需	《漏洞处理报告》
4	针对维保设备出现故障等问题，及时排查原因并处置，输出故障处理报告	按需	《故障处理报告》

信息系统硬件设备清单

序号	设备类型	设备名称	数量	使用年限
1	服务器	Dell PowerEdge R340 1台 Dell PowerEdge R740 3台 Dell PowerEdge R720 1台 Dell PowerEdge R930 1台	6	15
2	业务存储	Dell EMC DD2200 2台 Dell EqualLogic PS4210E 1台 Dell PowerVault MD3200 1台 VSP G350 2台	6	12
3	光纤交换机	新华三 HD6505 2台	2	12
4	网络安全产品	华为交换机 1台 山石网科防火墙 1台 H3C 防火墙 1台	3	10
5	中间机	世安 T5-A 3台	3	11
6	杀毒软件	江明 KV 企业版	1	4
7	数据库	SQL Sever 2014	1	4
8	操作系统	Windows Sever 2012 R2 数据中心版	3	4
9	UPS 不间断电源	UPS 不间断电源 2台	2	4
10	精密空调	泰恩特 2台 海信 1台	3	4
11	通风机	通风机	2	4

软、硬件原厂维保及授权

	设备类型	数量	品牌及型号
软件原厂维保服务	杀毒软件	1	江明 KV 企业版原厂病毒库升级服务（一年）
	数据库	1	SQL Sever 2014 标准版原厂服务（一年）
	操作系统	3	Windows Sever 2012 R2 数据中心版原厂服务（一年）
硬件原厂维保服务	HDS 存储	1台	VSP G350 1台
		1台	VSP G350 1台
		12块	神州云科 VSP 系列 12 块
		14块	神州云科 VSP 系列，14 块
		4个	神州云科 VSP 系列硬盘磁盘柜，4个
		2套	神州云科 VSP 系列 GAD 双活许可，2套
		1台	神州云科 VSP 系列， 1台
		30块	神州云科 VSP 系列，30 块
	中间机	1台	世安 T5-A
		1台	世安 T5-A
		1台	世安 T5-A

硬件运维备品备件

备件名称	备件数量	备件规格
R340 服务器硬盘	1	600GB 10K RPM SAS 12Gbps 2.5 寸
R340 服务器电源	1	350W
R740 服务器硬盘	1	600GB 10K RPM SAS 12Gbps 2.5 寸
R740 服务器电源	1	750W
R740 内存	1	32G ECC PC4 DDR4 2666
R740 主板	1	
R720 服务器硬盘	1	600GB 15K RPM SAS 12Gbps 3.5 寸
R720 服务器电源	1	750W
VNX5200 存储硬盘	1	4T 企业级 SAS 盘
VNX5200 存储电源	1	750W
MD3200 存储硬盘	1	4T 企业级 SAS 盘
MD3200 存储电源	1	600W
交换机	1	华为 S5735
精密空调滤芯	4	
精密空调冷凝风扇	1	
精密空调冷媒	1	冷媒 R22
UPS 蓄电池	1	12V100AH

服务团队人员表

序号	姓名	证书名称	级别	证号	项目中岗位	备注
1	施昌利	1. PMP 项目管理师证书 2. 高级网络工程师证	高级	1、3719453 2、C2301002A0301079	项目经理	无
2	陈登元	高级数据库管理工程师证	高级	C2301002A1000765	驻场工程师	无
3	生威	华为网络工程师	中级	01020271193809630852407465	驻场工程师	无
4	周辰宣	OCP 认证	中级	290454896DB19COCP	ITSS IT 服务工程师	无
5	张天淼	高级信息系统项目管理师证	高级	11101440119	高级信息系统项目管理师	无
6	李金文	高级软件工程师证	高级	C1201J02S3904861	高级软件工程师	无
7	孙迪迪	高级信息安全管理工程师证	高级	C2301002A1001071	高级信息安全管理工程师	无