

合同编号：

漯河市 X86 政务云运维服务和政务云
数据容灾备份服务项目
(A 包)
运维服务合同

项目名称：漯河市 X86 政务云运维服务和政务云数据容灾备份服
务项目 (A 包)

委托方（甲方）：漯河市行政审批和政务信息管理局

受托方（乙方）：中国联合网络通信有限公司漯河市分公司

签订日期：2025 年 1 月 6 日

签订地点：漯河市源汇区长江路 333 号

有效期限：2025 年 1 月 6 日至 2027 年 7 月 6 日

**漯河市 X86 政务云运维服务和政务云
数据容灾备份服务项目(A 包)
运维服务合同**

委托方（甲方）：漯河市行政审批和政务信息管理局

地 址：漯河市源汇区长江路 333 号

法定代表人/负责人：陈四新

项目联系人：崔子尚

联系方式：19037071314

通讯地址：漯河市源汇区长江路 333 号

电 话：0395-3177686

电子邮箱：lhsxjdzzwk@163.com

受托方（乙方）：中国联合网络通信有限公司漯河市分公司

地 址：漯河市郾城区嵩山路 316 号

法定代表人/负责人：邵水涛

项目联系人：张书恒

联系方式：15639501180

通讯地址：漯河市郾城区嵩山路 316 号

电 话：03953165139

电子邮箱：zhangsh195@chinaunicom.cn

本合同甲方委托乙方就“漯河市 X86 政务云运维服务和政务云数据容灾备份服务项目(A包)”进行专项运维服务，并支付相应的运维服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》以及相关法律法规的规定，达成如下合同，并由双方共同恪守。

第一条 运维服务内容

1. 运维服务内容：

乙方按照附件1的服务内容提供X86政务云运维服务：包括基础设施维保、云平台运维、硬件设备维保、软件运维、安全资源池软件授权、旧设备置换运维、其他运维等，按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《信息安全等级保护管理办法》《信息安全技术网络安全等级保护基本要求》《河南省非涉密政务信息系统安全建设指南（试行）》《漯河市政务信息系统安全运维一般规则》等法律、法规、技术规范及甲方需求提供运维技术服务，并配合甲方开展相关工作。并提供短信平台供所有 X86 政务云上云系统可使用全网短信服务，承担所有业务系统短信平台服务费（每月限额 30 万条短信，超出部分双方另行协商相关费用）。

2. 运维服务目标：

2.1 确保 X86 政务云的安全稳定运行；

2.2 保障运维质量，确保各方满意的运维成效。

3. 运维服务方式：委托方（甲方）委托受托方（乙方）为“漯河市 X86 政务云运维服务和政务云数据容灾备份服务项目(A包)”即“漯河市 X86 政务云”提供运维服务。双方签订运维合

同，受托方（乙方）按合同约定和委托方（甲方）要求开展相关运维事宜，并接受委托方（甲方）对运维工作的管理和考核。

第二条 运维服务实施范围和服务期限

1. 运维服务实施范围：包括基础设施维保、云平台运维、硬件设备维保、软件运维、安全资源池软件授权、旧设备置换运维、其他运维等。

2. 运维服务期限：服务周期 30 个月，自 2025 年 1 月 6 日至 2027 年 7 月 6 日。

3. 依据招标文件中项目商务条件约定，乙方应在中标通知书发出之日（2025 年 1 月 6 日）立即开展 X86 政务云运维服务工作。

第三条 合同费用及付款方式

（一）本合同乙方运维服务费用总额（含税价）为：11580000 元（大写：壹仟壹佰伍拾捌万元整），包括运维服务费用 9705000 元（大写：玖佰柒拾万零伍仟元整）（每月运维服务费用 323500 元乘以 30 个月），和旧设备置换费 1875000 元（大写：壹佰捌拾柒万伍仟元整），服务内容详见附件 1。其中旧设备置换费 1875000 元（大写：壹佰捌拾柒万伍仟元整）是指：若出现确需购置新设备或对旧设备更换情况，经甲方同意后，乙方须自行更换设备，必须保证系统正常运行，采购费用以乙方采购发票为准，据实结算，采购单价不得高于同期集中采购价格，运维服务期间采购费用整体不得超过 1875000 元（大写：壹佰捌拾柒万伍仟元整）。除本合同约定的运维服务费外，甲方不向乙方额外支付其他费用。

（二）原则上运维服务费支付周期为三个月。实际支付时根

据工作需要，经甲乙双方协商后，可变更支付周期。

绩效考核周期为一个月。运维服务每满一个月，甲方按照《漯河市 X86 政务云运维服务工作考核评价办法（试行）》（详见附件 2），结合乙方提供的考核资料和乙方工作实际情况，对乙方上月运维工作进行绩效考核。考核结果作为当月运维服务费用的结算依据。乙方应按照甲方要求及时提供考核资料，因乙方提供资料不及时或对考核工作不配合造成的不利后果由乙方承担。

具体支付方式如下：

每满一个支付周期，由甲方根据乙方绩效考核情况支付当期运维服务费，当期运维服务费计算方式为：每月运维服务费用×当期实际月数+当期实际产生的旧设备置换费-当期绩效扣除费用。

乙方根据绩效考核结果，每支付周期提供当期运维服务费对应金额的、符合国家规定的发票，经甲方核对后 30 个工作日内，支付对应金额。

（三）乙方银行账户信息和纳税人信息

乙方信息如下：

开户名：中国联合网络通信有限公司漯河市分公司

开户行：中国银行漯河分行营业部；

银行地址：漯河市郾城区嵩山路与黄河路口西北角；

账号：2481 0467 8485；

纳税人识别号：91411100729598668W；

第四条 考核标准

1. 绩效考核工作由漯河市行政审批和政务信息管理局负责并

委托漯河市政务大数据中心负责具体实施。

2. 绩效考核依据《漯河市 X86 政务云运维服务工作考核评价办法（试行）》等文件要求执行。

第五条 保密责任

（一）保密内容

1. 乙方对甲方提供的数据、文档、管理员账户等资料有保密的义务，不得将该资料和修改、转化后的资料用于其他用途。

2. 乙方不得向协议约定外的任何人、任何单位透露“漯河市 X86 政务云运维服务和政务云数据容灾备份服务项目（A包）”运维期间的相关信息数据，如用户信息、数据资源、技术资料等。

3. 履约过程中涉及涉密资料应按照相应的保密规定执行。

（二）涉密人员范围

与本合同项目相关人员，包括双方所有参与项目的技术人员、管理人员等；乙方应当为本合同所约定的甲方运维服务项目科学、合理地配置技术团队，在确保项目运维服务效果的基础上，严格控制本合同项目参与人员或信息接触人员。

（三）保密期限

本合同中的上述保密责任在合同终止后长期有效，相应的权利义务不因本合同的变更、解除或终止而消灭。

第六条 合同的变更、解除、终止

（一）合同的变更

本合同的变更必须双方协商一致，并以书面形式通知确定。

（二）合同的解除

双方确定，出现下列情形，致使本合同的履行成为不必要或

不可能的，可以解除本合同，且乙方应立即无条件将运维方案、运维日志、巡检报告、运维工单、本合同内运维服务涉及系统的完整源代码或最终安装部署包（确保用户数据可读取、可获取）、技术运维账号、服务期内项目采集存储数据等材料全量完整移交甲方且按照甲方要求配合完成运维交接工作，如不配合，甲方有权停止支付费用并追究乙方责任，期间产生的问题和造成的不利后果全部由乙方承担。运维交接工作完成前，运维责任仍由乙方承担。

1. 发生不可抗力（不可抗力指在合同履行过程中，不可避免、不能克服且不能提前防备的自然灾害和社会性突发事件等客观情况，如地震、台风、水灾、火灾、流行疾病、战争、政策变化等）；

1.1 不可抗力事件发生时，受阻方应立即通知对方，并在不可抗力事件发生后的十五日内提供有关该事件的公证文书和书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

1.2 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

1.3 如果不可抗力事件的影响持续达三十日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。

2. 乙方明确表示或以自己的行为表明不履行合同、或经甲方以书面形式通知其履约后仍未能依约履行合同、或以不适当的方式履行合同。

（三）合同的终止/中止

双方确定，当甲、乙双方因合同到期终止或某种因素中止合同时，乙方应立即无条件将运维方案、运维日志、巡检报告、运维工单、本合同内运维服务涉及系统的完整源代码或最终安装部署包（确保用户数据可读取、可获取）、技术运维账号、服务期内项目采集存储数据等材料全量完整移交甲方且按照甲方要求配合完成运维交接工作，如不配合，甲方有权停止支付费用并追究乙方责任，期间产生的问题和造成的不利后果全部由乙方承担。运维交接工作完成前，运维责任仍由乙方承担。

1. 合同期满：当合同的履行期限到达时，合同终止。

2. 合同目的实现或不可能实现：当合同的目的实现或者变得不可能实现时，合同中止。

第七条 所有权和知识产权

1. 在本合同有效期内，甲方利用乙方提交的服务工作成果所完成的新的技术成果，归甲方所有。

2. 在本合同有效期内，乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，归甲方所有。

3. 本合同生效时已经存在并为各方合法拥有或使用的技术、资料和信息，其知识产权和其他权益仍归原权利人所有。

4. 乙方保证其在本合同项下提供的服务不会侵犯第三方的知识产权和其他合法权益。如果甲方因接受乙方服务而侵犯第三方的合法权益，并因此涉入诉讼、仲裁或其他司法程序，乙方应就诉讼策略及其他事宜向甲方提供充分的支持与协助：如有生效的法律文书禁止甲方继续使用相关服务或要求甲方向第三人支付使

用费，乙方应采取相应的补救措施，并赔偿由此给甲方造成的全部损失。

第八条 违约责任

双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。出现违约情形的，违约方应停止违约行为，并按守约方的要求继续履行、采取补救措施或赔偿损失。

1. 如甲方未能按照本合同约定的期限向乙方支付相关费用的，每逾期[5]日，甲方应当按照当期运维费用的[1]%向乙方支付违约金。甲方已在约定付款周期内按照重大事项研究后，乙方同意该情形不视为甲方违约。

2. 乙方未能按本合同约定的期限按期提供运维服务的，每逾期[5]日，乙方应当按照当期运维费用的[1]%向甲方支付违约金。乙方逾期未提供服务累计达[30]日的，甲方有权单方解除本合同，同时乙方应向甲方支付本合同约定总金额[20]%的违约金，甲方因追讨欠费支出的各项费用（包括但不限于律师费、诉讼费、保全费、财产保全担保费等）由乙方承担。

3. 乙方承诺遵守国家相关法律法规，不进行危害项目安全的活动，若甲方发现乙方有危害网络安全的事项等活动，则甲方与乙方解除本合同甲方不负违约责任，本合同项下所有款项甲方有权向乙方追还，乙方应予以退还。

第九条 权利和义务

（一）甲方权利与义务

1. 甲方有权要求乙方按合同约定内容，保质保量完成交办的服务事项。

2. 在合同约定的服务期限内，甲方对乙方的运维服务行为、服务内容、服务质量进行监管和评价，有权对乙方的服务事项提出整改要求。

3. 甲方有权要求乙方在合同期内分享合同约定的服务事项相关技术问题的知识、经验、方法。

4. 本项目的绩效考核工作按照《漯河市 X86 政务云运维服务工作考核评价办法（试行）》开展，考核认为项目运维工作未达到预期效果的，甲方有权按照绩效考核方案要求对乙方处以限期整改、扣除运维资金等处罚措施。

5. 甲方应按本合同约定，向乙方支付合同款项。

（二）乙方权利和义务

1. 乙方有权对本合同内相关运维工作提出合理化建议。

2. 乙方有权就合同期间甲方的侵权或违约行为，采取法律手段维护自身权益。

3. 乙方应提供服务以纠正、修复系统缺陷，且由此引起的额外费用全部由乙方承担。

4. 乙方除保证项目运维安全稳定运行、系统免费优化外，应向甲方提供项目涉及到的软、硬件相关技术服务支持并且按照甲方需求开展安全培训，提高安全意识和安全操作技能，包括但不限于项目运维过程技术人员的现场指导，对项目定期检测、维护、漏洞修补、升级改造及运营过程中可能出现的其他问题的维护和优化。

5. 除本合同内约定的运维服务内容以外，因新增需求而导致新增运维内容，需先由相关方提出正式需求文件后甲方和乙方共

同进行评估，如确认新增需求，相关费用由甲乙双方另行协商解决；但因上级要求或相关法规变更造成的新增运维内容，原则上由乙方免费进行保障。

6. 乙方应在合同生效期间，向甲方提供运维工作产生的运维管理员账号。

7. 乙方应按照甲方的要求开展日常运行维护工作，组建专业运维团队，明确具体责任人员，及时将分工情况和工作进展情况告知甲方，承担约定的运维服务职责。

8. 乙方应按照国家法律法规、网络安全等级保护、安全技术标准等，建立“漯河市 X86 政务云运维服务和政务云数据容灾备份服务项目”运维实施方案，经甲方审议通过后施行，并采取相应技术措施，加强网络安全管理，建立执行层面的应急处置预案、定期组织应急处置演练，做好 7*24 小时运维保障工作。保障“漯河市 X86 政务云运维服务和政务云数据容灾备份服务项目（A 包）”内各运维事项的安全稳定运行，落实网络和数据安全直接责任。

9. 乙方负责项目出现突发性故障时，应按照故障等级进行响应，排查原因、解除故障并出具问题分析报告；出现漏洞时，高危漏洞，乙方需立即处理，中低危漏洞，应在 24 小时内处理。故障和漏洞处理结束后，乙方应向甲方提交盖有公章的书面报告，因客观原因无法处理的故障和漏洞，也应及时向甲方提交盖章的书面报告。

10. 乙方为本项目的授权实施方，在合同服务期内应当负责运维服务质量，保障项目稳定运转，因乙方运维服务问题导致项目

运行出现故障的，乙方应当在甲方规定时间内予以修复、维护，否则甲方有权要求乙方承担相应的责任。

11. 乙方应在合同期满后 7 日内，无条件将运维方案、运维日志、巡检报告、运维工单、本合同内运维服务涉及系统的完整源代码或最终安装部署包（确保用户数据可读取、可获取）、技术运维账号、服务期内项目采集存储数据等材料全量完整移交甲方，且按照甲方要求配合完成运维交接工作，如不配合，甲方有权停止支付费用并追究乙方责任，期间产生的问题和造成的不利后果全部由乙方承担。运维交接工作完成前，运维责任仍由乙方承担。

12. 乙方负责在合同生效运维期间，配合将项目产出的数据资源目录全量纳入市政务数据共享交换平台统一发布、挂载、运行管理，建立完善数据质量闭环管理、数据更新、共享数据使用情况反馈机制，确保数据供给质量，根据甲方业务协同、数据共享等需求，免费提供与第三方系统的对接和数据推送服务。

13. 乙方应根据甲方实际需求，定期按要求向甲方提交运维日志，运维工作报表等，此项纳入甲方对乙方工作考核范围内。

14. 乙方应根据甲方实际需求，对确需购置新设备或对旧设备更换情况，乙方须自行更换设备，必须保证系统正常运行，购置费用以采购发票为准，据实结算，采购单价不得高于同期集中采购价格，运维服务期间整体不得超过 1875000 元，超过部分由乙方自行承担。

15. 乙方应根据甲方实际需求，按照省一朵云综合管理平台对接标准，持续向省平台按标准推送数据。

16. 乙方应根据甲方实际需求，待漯河信创云服务采购完成

后，按照甲方需求免费配合完成信创替代。

17. 为保障政务云服务的持续性，原则上乙方应依托现有机房开展运维工作，若发生机房搬迁，乙方应保证网络环境不发生变化，云平台及平台承载的业务系统不得中断，由此产生的一切费用将由乙方自行全部承担。

18. 乙方应按照甲方需求免费提供对存量宿主机以及云上centos 操作系统进行安全加固，以满足相关部门要求。

第十条 合同联系人

甲乙双方因履行本合同或与本合同有关的一切通知都应当按照本合同中的联系人、地址，以书面信函或者电子邮件方式进行。其中：

（一）双方确认，在本合同有效期内，合同双方联系人通知地址及方式如下：

甲方：漯河市行政审批和政务信息管理局

地址：漯河市源汇区长江路 333 号

联系人：崔子尚

电话：0395-3177686

邮编：462000

电子邮箱：lhsxjdzzwk@163.com

乙方：中国联合网络通信有限公司漯河市分公司

地址：漯河市郾城区嵩山路 316 号

联系人：张书恒

电话：15639501180

邮编：462000

电子邮件：zhangshl195@chinaunicom.cn

（二）除本合同另有约定外，有关下述任一事项的通知，均应当采用书面信函形式作出，否则，该通知无效，不产生本合同项下的任何通知效力：

1. 与本合同费用及支付事宜有关的通知。
2. 与本合同违约事宜有关的通知。
3. 与本合同终止/中止、解除或变更事宜有关的通知。
4. 与本合同延续/续展有关的通知。

如果因接受方原因（包括但不限于接受方拒收书面信函、联系方式变更、接受方电子邮箱地址不存在或者邮箱已满或者设置拒收等）导致通知发送失败，视为通知已经送达（发送方侧载明的书面信函寄出时间或者电子邮件发送时间视为通知送达时间）。

上述任何信息发生变更的，变更方应当及时以书面形式通知另一方，未及时通知并影响本合同履行或造成损失的，应当承担相应的责任。

第十一条 安全与责任

1. 甲方对本合同项目的网络和数据安全负有监督责任。乙方确保项目的网络数据安全得到有效维护和管理。

2. 乙方是本合同项目网络和数据安全的直接责任方，负责运维过程中的网络和数据安全具体工作，承担安全管理职责，保障项目的安全稳定运行。

3. 乙方需按照国家、省、市法律法规和《漯河市政务信息系统安全运维一般规则》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《互联网政务应用安全管理规定》《河南

省政务云管理办法》《漯河市政务云管理暂行办法》关于网络和信息安全有关规定开展运维活动。同时，遵守政务云相关的国家标准，如 GB/T34080.3-2021《信息安全技术基于云计算的电子政务公共平台安全规范》，确保运维工作符合国家及地方的法律法规要求，有效保障政务云平台的信息安全。

4. 乙方需对运维人员进行安全意识教育和岗位技能培训，包括但不限于安全基础知识、岗位操作规程等，并告知相关的安全责任和惩戒措施。

5. 乙方需加强运维人员安全管理，进行岗前背景审查，重点排查是否有网络安全事故记录，国（境）外学习工作经历，外籍、境外居留权、长期居留许可等方面情况。并与甲方及相关人员签订保密协议和安全岗位职责协议。

6. 合同期满后，未经甲方许可，乙方不得私自留存或使用项目数据和账号。

7. 因乙方原因造成的安全问题或事故，损失由乙方承担；给甲方造成不利影响的，乙方应当及时挽救并对甲方的损失予以赔偿。

第十二条 法律适用和争议解决

（一）本合同适用中华人民共和国法律。

（二）所有因本合同引起的或与本合同有关的任何争议通过双方友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。如果在一方提出协商要求后 7 日内，双方不能通过友好协商解决争议，则任何一方均可向甲方住所地有管辖权的人民法院起诉。

(三) 诉讼进行过程中, 除双方有争议的部分外, 双方继续履行本合同未涉及诉讼的其他部分。

第十三条 其他

(一) 任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同做出的任何修改和补充应为书面形式, 由双方签字盖章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时, 以补充合同或者补充协议为准。

(二) 本合同附件及补充协议均是本合同不可分割的一部分, 具有同等法律效力。

(三) 本合同一式肆份, 甲乙双方各执贰份, 具有同等法律效力。

(四) 未经另一方书面同意, 任何一方不得转让本合同项下任何权利义务。

(五) 本合同经甲乙双方签字盖章后生效。

第十四条 本合同附件

附件 1: 漯河市 X86 政务云运维服务和政务云数据容灾备份
服务项目服务内容

附件 2: 漯河市 X86 政务云运维服务工作考核评价办法 (试行)

合同签署页（以下无正文）

甲方（盖章）：
法定代表人/委托代理人（签字）：郭厚水
签署日期：2025年01月17日

乙方（盖章）：
法定代表人/委托代理人（签字）：王明生
签署日期：2025年1月6日

附件 1 服务内容：

X86 政务云运维服务：包括基础设施维保、云平台运维、硬件设备维保、软件运维、安全资源池软件授权、旧设备置换运维、其他运维等。

1. 云平台运维服务

需提供完善的技术服务及运维保障服务，包括资源监测、资源配置、资源优化、服务监测、事件处理、运维流程、日常巡检、备份恢复、应急预案管理、服务质量报告等服务。乙方应针对漯河市政务云机房的维护管理、运维操作、应急管理以及云服务的申请、交付、保障、监督等流程制定相关规范和标准，并根据实际运行需求进行持续更新和优化。

乙方应具备对全部 IT 物理设备（包括服务器、网络、存储和安全设备等）、虚拟机、操作系统（Windows 和 Linux）的监测能力，能够输出监测对象的监测数据信息。

乙方应根据本项目的特点，建立完备运维管理体系，标准规范的运维管理制度，明确项目组织管理措施和手段。具备对日常运维管理事务的支撑，包括服务台、事件管理、问题管理、变更管理、资产管理等服务管理机制，并根据管理需求的变化进行必要的更新，确保项目实施和运维服务的有效性和服务团队的稳定性。

乙方未经政务云管理单位允许不得对云系统使用云资源进行变更，如需变更，必须经政务云管理单位同意。

乙方未经允许不得对云平台上的任何数据进行截取、加

工、分析和处理，或提供给第三方。

上云业务单位有系统迁出需求时，乙方应无条件配合政务云管理单位完整迁出应用系统。

乙方配合全市各单位应用系统迁移前的环境需求分析工作。负责全市各单位应用系统迁移前的测试环境搭建工作；配置物理服务器、配置虚拟机、配置网络、配置相应的安全策略等。

乙方应提供根据用户需求按照政务云规定流程对用户云资源 CPU 核数、内存空间、硬盘、网络 IP 地址以及安全防护服务等配置进行变更。

乙方应制定规范的服务巡检制度，定期针对机房基础设施、基础 IT 设备、运维支撑平台、关键业务系统进行定时巡检，及时发现系统故障及安全隐患。

在重要关键时刻，包括重大会议期间、网络重大割接或其它任何可能对网络业务产生重大影响时刻，提供专人现场值守。

运维输出物：

①. 云平台配置管理，协助记录、更新、管理云平台基础信息、账号信息、常用配置信息及云平台拓扑信息，每月月末提供 1 次《云平台配置文件》。

②. 云平台运维：开展对云平台系统所有相关软件基础环境、组件、产品进行运维，包括基础服务监控、系统故障处理、系统日志检查和诊断、业务单位需求统计等涉及云平

台安全稳定运行的其他服务，每周周日之前提供《政务云平台运维周报》。

③. 日常监控巡检：对云平台产品可用性进行监控，保证云平台问题和异常情况的有效及时发现并通知。对服务器设备、网络设备、存储设备的运行状态每天开展轮训巡检，对其正常与否、健康程度进行数据化的评价和判定。开展基础应用巡检、管控平台巡检、产品巡检，每天早晚各 1 次，每周周日之前提供《政务云巡检周报》。

④. 资源管理：根据要求开通、变更、释放云资源，云资源交付周期不多于 2 个工作日。定期整理输出云资源清单和云资源利用率统计表。每周周日之前提供《政务云云资源统计表》，每月 5 号之前提供《政务云业务系统云资源利用率统计表》。

⑤. 事件管理、应急响应：对云平台提供全生命周期的问题排查、诊断、定位和修复，直至恢复云产品和业务的运行正常；记录、更新平台发生的突发事件/事故，定期总结分析，重大事件协调人员现场解决，并根据原因统计分析给出流程、技术上的改进建议。事件管理包括事件级别、事件类别、发生时间、事件描述、影响范围、应急处理、处置结果、整改建议等，云平台运维事件处理记录每周汇总 1 次提供《云平台运维事件处理记录》；对于重大事件，定位后在 5 个工作日之内输出《云平台信息安全事件报告单》。

⑥. 故障管理：记录、更新云平台的故障和处理方法，

每月汇总分析，提供《政务云平台故障处理报告》。

⑦. 平台应急演练：对灾难故障模拟演练提供技术支持，包含演练方案规划设计、业务恢复方案以及演练总结。确保云平台出现信息安全事件的及时阻止与业务恢复，避免同类信息安全事件的再次发生或降低发生后的影响，提升运维团队应急处理能力。每年开展 1 次应急演练，提供《政务云演练方案》和《政务云演练报告》。

2. 网络安全运维服务

① 驻场运维要求

驻场人员需具备网络基础巡检能力、网络资产探测能力、设备配置核查能力、日志分析能力、安全事件分析能力及安全事件处置能力等；

乙方主要负责网络安全产品管理、日常巡检、日志审计与分析、网络通报、重保值守服务、管理制度体系建设、策略配置优化、配置备份、网络安全培训等服务工作，

交付物：《运维服务报告》

② 网络安全产品管理

运维 27 台网络安全产品和 2 套网络安全资源池，包括但不限于防火墙、入侵防御、入侵检测、VPN、安全运维堡垒机、漏洞扫描、日志审计、跨网数据安全交换系统等网络安全防护设备及设施；

通过人工手段、空间资产测绘手段及其他资产发现手段，对安全产品进行梳理摸底、登记造册，形成资产清单，

包括设备编号、设备名称、设备厂家、产品型号、IP 地址、端口开放情况、物理位置、连接关系、访问关系、责任人、使用人、数据流等基本信息梳理和核对；

对资产清单中的资产按照梳理情况，绘制网络结构拓扑图和立体资产结构图，定期完善更新；

按照等级保护和关键信息基础设施基本要求，对安全产品进行合规管理，包括但不限于：所有资产的控制权限管理、日常运维操作管理及基线防护管理等；

对资产管理用户权限进行定期巡检和收敛，对网络安全产品定期进行密码修改；

交付物：《资产信息统计表》、《资产密码变更记录表》、《网络结构拓扑图》；交付频次：一次/月，发生变更时及时补充。

③安全保密策略配置管理

安全防护策略管理，包括但不限于梳理网络访问控制、角色权限控制、账号授权策略现状，分析高风险策略、高权限泄露以及帐号权限授权策略等存在的安全风险，针对存在的安全防护策略问题出具对应的整改通告单；

针对全局性策略，应实现网络整体防护全局配置，重点对有效性、覆盖性、重复性和确实性策略进行巡检；

针对专项性策略，应按照明确的 IP 五元组（源 IP、源端口、目的 IP、目的端口、服务协议）实现配置；

针对防护性策略，定期通过安全日志进行巡检和分析，并配

置针对防护对象的策略；

针对权限策略，定期巡检资产相关联的用户管理权限，并对权限合法性和有效性进行验证；

定期对异常策略配置，研判后做出决策；

交付物：《全局性访问控制策略清单》《专向性访问控制策略清单》《防护性策略清单》《权限策略清单》《安全防护策略问题整改通告单》等；交付频次：一次/月，发生变更时补充。

④网络安全产品巡检

针对网络安全产品开展本地巡检服务；

巡检内容包含但不限于对网络安全产品的硬件运行状态、CPU 利用率、内存利用率、存储空间利用率、接口、事件告警、日志记录、特征库版本等完成巡检工作，重点对异常情况进行分析并上报；协助安全产品乙方完成整改并跟踪记录，完成巡检闭环；

交付物：《安全产品日常巡检记录表》、《安全产品问题整改通告单》；交付频次：一次/周。

网络安全通报

定期收集云上资产安全漏洞，及时进行安全通报并配合后续的修复漏洞工作，第一时间降低资产脆弱性，完成通报闭合；

交付物：《资产安全通告》；交付频次：一次/周进行，重保时期一次/天。

⑤安全配置优化

以网络安全等级保护基本要求和关键信息基础设施基本要求为依据，包含但不限于对设备的基线配置策略、网络安全访问控制策略、网络安全防护策略和网络安全审核策略进行配置优化；对边界防护策略进行实时动态调整和优化；交付物：《安全产品配置策略优化单》；交付频次：一次/周，发生变化时和重保时期随时更新。

⑥重大活动安全保障

重要时间节点、重大节假日期间，确保及时处置网络安全隐患，充分做好人员、技术、服务等安全保障工作，尽可能避免出现黑客攻击入侵、篡改事件、感染受勒索病毒等安全风险，提供强大网络安全支撑能力。保障结束后出具相关的保障总结材料；

按照重保活动要求，完成但不限于：重保前的准备活动（检测和加固等）、重保过程中值守活动（巡检、防护、值守、研判及处置活动）、重保完成后的总结活动等；保活动保障期间，需配备必要的专家服务团队为现场值守人员提供支持保障；

交付物：《重大活动保障总结报告》；交付频次：按需进行。

3. 网络安全资源池服务

依托现有搭建的云安全资源池平台软件两套，提供防火墙、WEB 应用防火墙、堡垒机、数据库审计、日志审计、漏

洞扫描、主机安全管理等安全资源服务。明确平台、租户责任边界，划清网络安全主体责任。实现安全可视、可控、资源自动化部署、弹性扩展、平台开放等功能，形成云内安全事件防护闭环。

①防火墙安全组件服务

驻场运维人员针对云租户需求进行策略开通、优化、管理等服务；协助云租户对防火墙安全组件进行管理，对安全事件进行上报工作。

②WEB 应用防火墙安全组件服务

驻场运维人员针对云租户需求进行规则配置、优化、管理等服务，针对云租户 WEB 应用的防护日志、防护站点、站点流量等内容进行监测；协助云租户对云 WEB 应用防火墙安全组件进行管理，对 WEB 应用安全事件进行上报工作。

③堡垒机安全组件服务

驻场运维人员日常针对运维权限开通、运行维护等内容进行技术支撑；协助云租户按照需求对云运维审计安全组件服务进行管理，对运维事件进行分析和溯源工作。

④数据库审计安全组件服务

驻场运维人员日常针对日志接收情况、日志告警进行监测，提供日志接入的技术支撑；协助云租户按照需求对云数据库审计安全组件服务进行管理，进行事件告警上报工作，以及协助对异常行为的审计取证。

⑤日志审计安全组件服务

驻场运维人员日常针对日志接收情况、日志告警进行监测，提供日志接入的技术支撑；协助云租户按照需求对云日志审计安全组件服务进行管理，对告警事件进行上报工作。

⑥漏洞扫描安全组件服务

驻场运维人员每季度针对云租户资产的弱口令、端口、服务、漏洞等内容进行检测服务。协助云租户协助云租户对漏洞扫描组件进行管理，对各类漏洞进行上报工作，协助完成漏洞修复后的回归性扫描工作。

⑦主机安全管理组件服务

驻场运维人员每日针对云主机病毒查杀、木马查杀、主机防护等内容进行监测及整理；协助云租户对云主机安全管理组件进行管理，对主机安全事件进行上报工作。交付物：《云租户资产对接申请单》、《系统运维月度综合分析报告》、《业务系统漏洞扫描季度报告》。

⑧重保、攻防演练及成果汇报服务

提供春节、清明、五一、国庆等国家法定节假日和重要时期的保障工作（如，国家/省/市“两会”、国内重要活动等重要时期），制定专项保障服务措施及方案，提供 24 小时的安全专家级保障与监测，包括但不限于对云安全管理平台服务情况进行监控、安全配置加固、安全监测、应急响应处置等服务；提供如公安部、省/市公安组织的“HW”演练等活动的保障工作，提供 24 小时安全专家级保障服务，包括但不限于活动前的安全方案支持、活动过程中的监控预警

以及突发事件的研判应急和活动后的服务资料总结提交；运维人员按照服务内容编写日报，详细记录服务对象的运行情况、告警情况、攻击事件、审计日志等内容，并截图留存；运维人员结合本周日报以及运维事项等内容编写周报，记录服务对象本周的运维概况与运维事件，重点阐述本周内各项安全事件、防护情况等内容；交付物：《驻场人员工作日报》《驻场人员值班表》等。

4. 硬件设施的运维保障服务

①设备巡检工作

开展对基础平台服务的物理信息化硬件进行巡检，每天2次，“重保”等特殊时期，每天4次。巡检人、巡检内容、巡检结果等信息应有对应的纸质文档记录。

②运行监控工作

通过对设备的监控，及时发现并记录异常信息，探索设备的运行规律。当出现故障时，能及时报告和处理，保持设备的高效运行。监控对象为云平台的硬件设备，监控周期分为每日、每周或每月。根据监控结果，做好运行监控情况记录，填写各类巡检单。

进行监控管理的内容包括：

物理服务器和虚拟机的CPU性能管理；

物理服务器和虚拟机内存使用情况管理；

物理服务器和虚拟机硬盘利用情况管理；

物理服务器和虚拟机性能管理；

实时监控物理服务器电源、风扇的使用情况及主机机箱内部温度；

监控物理服务器硬盘运行状态；

监控物理服务器网卡、阵列卡等硬件状态；

③故障管理工作

在硬件故障发生后，应及时响应、迅速定位、稳妥解决，尽快恢复正常的服务，将负面影响降到最低。并通过对故障处理的记录、分析和总结，形成知识库案例，提出优化建议或改进措施。

④分析与报告整理工作

通过对日常运行监控、故障处理等运维记录的收集、整理、汇总，形成《云平台月度运行监控月报》。详细描述云平台每月的总体情况、变更情况、故障处理情况。

5. 机房运维要求

定期对机房环境巡检，定期对机房供配电、空调、温湿度控制等设施进行维护管理；制定《机房安全管理制度》对机房的物理访问和物品带进带出机房做出规定。指定专业部门每天对信息系统相关的设备与线路进行维护管理。制定《运行维护管理办法》，对设备维护进行有效的管理；定期执行漏洞扫描，对系统存在的已知漏洞就进行发现，经过测试通过后进行漏洞修补；制定《安全事件管理办法》，包括安全事件定义，安全事件分类、安全事件对业务造成的影响程度、组织职责、安全要求等内容。制定《信息安全-安全

事件处理流程》，确定安全事件的程度，安全事件的响应和处理流程等。制定《应急技术安全规范及预案》，规定各业务系统应急计划需要在单位信息安全管理部门批准后对计划中设计的相关人进行培训。定期对应急预案进行演练，提供应急处置能力。

6. 驻场服务

为确保政务云平台上相关系统运行正常，实行人员本地化、服务本地化，提供专业的服务保障团队，包括但不限于、项目经理、云计算工程师、网络工程师、网络安全工程师、运维工程师专家，并协助建立配套的标准规范、风险控制、运营管理体系，服务乙方委派至少 6 名驻场运维人员提供 7*24 小时驻场运维服务；并且定期向相关部门提交运维报告。

人员驻场服务包括规范性日常维护，故障应急响应，安全事件处置、设备问题解决等范围，包括但不限于以下内容：云平台的资源监测、资源配置、资源优化、网络安全策略配置、服务监控、事件处理、运维流程、日常巡检、备份恢复、安全管理、应急预案管理、服务质量监督和报告、协调相关单位等。

7. 故障应急响应服务

根据故障的严重程度和影响程度的不同，制定不同级别故障响应服务，保障故障的及时响应和处理。

故障级别	响应时间	故障解决时间
------	------	--------

I 级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失。	10 分钟，30 分钟内提交故障处理方案	2 小时以内
II 级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	10 分钟，30 分钟内提交故障处理方案	6 小时以内
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。	10 分钟，30 分钟内提交故障处理方案	12 小时以内
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	10 分钟，2 小时内提交故障处理方案	24 小时以内

8. 运维设备服务清单

政务云机房总共 64 组机柜空间，其中电源柜 4 组空间，空调柜 8 组空间，承重墙 2 组空间，实有 50 组机柜空间。

目前 X86 政务云平台配备机柜 40 组，共有政务云设备 299 台，其中计算和存储设备 211 台、交换设备 60 台、安全设备 28 台，承载了 39 个市直单位的 109 个政务信息系统，已使用云主机 913 台、物理机 21 台。

（实际运维设备服务清单最终以经双方确认的书面函

件为准，运维服务期间新增的设备一律免费纳入运维设备服务清单，运维服务商除此清单以外还需保障其他有关单位托管于政务云机房的设备运维。）

序号	设备厂家	型号	硬件配置信息	数量
1	H3C	UniServer R4300 G3	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 32GB*10 硬盘 SATA HDD 12T*24 SATA SSD 480G*2 SATA SSD 960G*6RAID-P460-M4CNA-10GE-2P-56 0F-B2-1*2 NIC-GE-2P-360T-B2-1-X*1 NIC-GE-4P-360T-L2*1	9
2	H3C	R4900G3	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 32GB*12 硬盘 SATA SSD 480G*2RAID-P460-M2NIC-GE-4P-360T-L 3*1	15
3	H3C	R4900G3	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz*2 内存 DDR4 2933MHZ 32GB*12 硬盘 SATA SSD 480G*2RAID-P460-M2NIC-GE-4P-360T-L 3*1	7

4	H3C	R4900G3	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz*2 内存 DDR4 2933MHZ 32GB*12 硬盘 SATA SSD 480G*2RAID-P460-M2NIC-10GE-2P-520 F-B2-1-X*2 NIC-GE-4P-360T-L3*1	2
5	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4214 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 16GB*16 硬盘 SAS HDD 600GB*2 SATA HHD 8T*10 SATA SSD 960G*2RAID-P460-M2NIC-GE-4P-360T-L 3*1	9
6	华为	HUAWEI Tecal RH2288H V2	intel E5-2650 v2 2.60 GHz*2、内存 DDR31333MHz 16GB*12、硬盘 SAS HDD 600G*4、LSI 2208 RAID 卡、千兆网卡 I350*1	52
7	华为	HUAWEI 2288H V5	CPU: 2*intel(R)xeon(R)silver4114cpu2.2GHz、内 存: 32*8GB (256)、硬盘: 600G SAS 系统 盘 2 块 960G SSD 固态盘 2 块 8T SAS 数 据盘 10 块 、RAID:LSI SAS 3108	10
8	超聚变	2288HV5	intel 4214 2.4GHz*2、内存 DDR4 2400MHz 32GB*2、硬盘 SATA SSD	2

			960G*3、SAS3108 RAID 卡、千兆网卡 I350*1、万兆网卡 Intel 82599*1	
9	超聚变	2288HV5	intel 4214 2.4GHz*2、内存 DDR4 2400MHz 32GB*2、硬盘 SATA SSD 480G*3、SAS3108 RAID 卡、千兆网卡 I350*1、万兆网卡 Intel 82599*1	2
10	超聚变	2288HV5	intel 4214 2.4GHz*2、内存 DDR4 2400MHz 32GB*2、硬盘 SATA SSD 240G*2、SAS3108 RAID 卡、千兆网卡 I350*1、万兆网卡 Intel 82599*1	2
11	浪潮	NF5280M5	Xeon(R) Silver 4216 2.1GHz*2、内存 DDR4 2400MHz 32GB*8、硬盘 SATA HDD 4T*6、千兆网卡 Intel*4、万兆网卡*4	11
12	超聚变	XFUSION 2288H V5	intel 4210 2.2GHz*2、内存 DDR4 2933MHz 32GB*12、硬盘 SATA SSD 480G*2、XR450C RAID 卡、千兆网卡 I350*1、万兆网卡 Intel 82599*1	20
13	H3C	UniServer R4900 G3	intel 4210 2.2GHz*2、内存 DDR4 2933MHz 32GB*12、硬盘 SATA SSD 480G*2、SAS HDD 1.2T*3、RAID 卡*1、 网卡*4	3

14	华为	HUAWEI Tecal RH2288H V2	Intel(R)Xeon(R)CPUE5-2650v2@ 2.60GHz*2、内存 DIMM000,Samsung,16384 MB,1600MHz*12、硬盘 SAS 600G *4、RAID 卡 L5I SAS2208	7
15	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 64GB*6 硬盘 SATA SSD 480G*2RAID-P460-M2NIC-10GE-2P-520 F-B2-1-X*2 NIC-10GE-2P-560F-L2*1	20
16	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 32GB*12 硬盘 SATA SSD 480G*2RAID-P460-M2CNA-10GE-2P-56 0F-B2-1*2 NIC-GE-4P-360T-L3*1	15
17	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4214 CPU @ 2.20GHz*2 内存 DDR4 2933MHZ 16GB*16 硬盘 SAS HDD 600GB*2 SATA HHD 8T*10 SATA SSD 960G*2-NIC-GE-4P-360T-L3*1	1
18	华为	HUAWEI Tecal RH2288H V2	Intel(R)Xeon(R)CPUE5-2650v2@2.60GHz *2、硬盘 SAS 600G *4、L5I SAS2208RAID	1

			卡	
19	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz*2, 内存 DDR4 2933MHz 64GB*6, RAID-P460-M2 , 6 Gbps SATA SSD 480GB*2, 12 Gbps SAS HDD 2.4TB*2	2
20	H3C	R6900G3	Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz*4,内存 DDR4 2933MHz 64GB*16,RAID-LSI-9361-8i(2G)-1-X,6.0 Gbps SATA SSD 480GB*2	4
21	H3C	CF9945	48 块 3.84TB SW SFF SSD	1
22	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz*2, 内存 DDR4 2400MHz 32GB*12, RAID-P460-M2, 硬盘 SATA SSD 480G*2, 硬盘 SAS HDD 4TB*2	6
23	华为	RH2288HV3	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz*2, 内存 DDR4 2933MHz 32GB*10, LSI 3108 RAID 卡, 硬盘 SATA SSD 960G*3, 硬盘 SAS 600G*12	2
24	H3C	UniServer R4900 G3	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz*2 内存 DDR4 2933MHZ 32GB*12 硬盘 SATA SSD 480G*2RAID-P460-M2NIC-10GE-2P-530	1

			F-B2-1-X*2 NIC-GE-4P-360T-L3*1	
25	超聚变	2288HV5	CPU:4214R 2.4GHz *2、内存: DDR4 2400MHz 32G*2、硬盘: SSD SATA 960G*3、 RAID 卡: SAS3108	1
26	超聚变	2288HV5	Intel(R) Xeon(R) Silver 4116 CPU @ 2.10GHz*2, 内存 DDR4 2933MHz 32GB*4, LSI 3108 RAID 卡, 硬盘 SATA SSD 480G*2, 硬盘 SATA SSD 960G*3	4
27	爱数	AnyBackup Enterprise 7	一体机主模块, 机架式 2U12 个 3.5 英寸盘 位设备 (最大可配置 12 块 7200 转 3.5 英 寸硬盘), 标配双路 Intel 4210 2.2GHz 10core CPU; 标配 256GB 内存 (8*32GB 3200MHz DDR4 内存, 剩余 22 个可用内 存插槽); 标配 2*960G SSD 盘做系统盘; 标配 4 个千兆网络端口和 2 个万兆光口 (含光模块); 空闲 5 个 PCIe 扩展槽 (支 持 8GB 或 16GB FC HBA 卡, 1GE 或 10GE 网络接口卡)。32GB 高速缓存 (3200MHz)32GB/DDR4/ECC/3200MHz*6 , 双口万兆网卡 光纤接口 10000Mbps/PCI-E/FCoE/双口/含 2 个多模	2

			光模块*1, NLSAS 12TB 硬盘 3.5 寸 7200 rpm/256M 缓存/*12。	
28	H3C	S5820V2-52QF	48 个 SFP Plus 端口,4 个 QSFP Plus;3 个 40G 光模块;	8
29	H3C	S6860	48 个 SFP Plus 端口,6 个 QSFP Plus 或 2 个 QSFP28 端口	14
30	H3C	S5130	48 个 10/100/1000BASE-T 电口,4 个 1G/10G BASE-X SFP+端口,支持 AC; 2 个万兆多模光模块	2
31	H3C	S5800	48 个电口,4 个光口,2 个 10G 光口	6
32	H3C	S9810	交换容量 43Tbps,2 个主控板,2 个交换网板,4 个 24 端口 10GE 光接口	2
33	H3C	ns316x	16 个 1/10G BASE-X SFP+端口	2
34	网御星云	Leadsec-DC-33 50	硬件形态: 标准机架式机箱, 双服务器主机架构, 专用安全加固 Linux 操作系统, 冗余电源。 内网接口: 配 1 个 100/1000M Base-TX 管理接口, 1 个 10000M SFP+多模网闸接口, 1 个 10000M SFP+多模网络接口, 1 个	2

			100/1000M Base-TX 网络接口。 外网接口：配 1 个 100/1000M Base-TX 管理接口，1 个 10000M SFP+多模网闸接口，1 个 10000M SFP+多模网络接口，1 个 100/1000M Base-TX 网络接口。 软件系统：配设备管理系统；配置请求与响应交换模块，含系统集群模块以及集群配置器，实现负载均衡和热备功能，含请求与响应模块，双网闸热备数据模块。 性能:交换能力：4000Mbps；最大支持服务 60 个。	
35	网御星云	SIS-3000-Z8100	双冗余电源;内网接口:4 个 10/100/1000M 自适应网络口，1 个管理口和 HA 口;4个SFP 光模块插槽,4个 SFP+万兆光口插槽(不包含光模块);2 个 USB 口;1 个串口;外网接口:4 个 10/100/1000M 自适应网络口，1 个管理口和 HA 口;4个SFP 光模块插槽,4个 SFP+万兆光口插槽(不包含模块);2 个 USB 口;1 个串口。配置 4 个万兆多模光模块。	3

36	网御星云	Leadsec-CM-3500/Leadsec-CMD-1000	硬件形态：标准机架式机箱，专用安全加固 Linux 操作系统，冗余电源，网络接口：4 个 100/1000M Base-TX 网络接口。软件系统：标配设备管理系统，其中有管理数据交换链路、管理单向导入链路和管理视频交换链路三种授权模块，硬件形态：标准机架式机箱，专用安全加固 Linux 操作系统。网络接口：6 个 100/1000M Base-TX 网络接口。1、支持采集多种设备的运行状态信息；2、支持对多种设备的流量信息采集；3、支持 SYSLOG 协议；4、支持 SNMP v2/SNMP v3 协议；产品服务：三年产品维修服务，包含三年硬件保修、5×8 技术支持服务。	2
37	H3C	H3C SecCenterCSAP-SA-M	CPU Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz *1；内存 16G 2666MHz DDR4 HMA82GR7AFR4N-VK Hynix Semiconductor 2 条；网卡 NIC-GE-4P-360T-L3 *1；电源 1 个 PSR550-12A，风扇 4 个 3203A01V；硬盘 4T*3	2
38	网御星云	TS-SC-S1100	冗余电源，配置千兆电口≥4 个、千兆光口≥2 个，不限 IP，最大并发扫描 100 个，冗余电源	2

			提供三年硬件保修和三年应用特征库升级服务。	
39	网御星云	LA-OS-6600-S	运维资源授权数量 150 个, 支持图形协议并发运维数≥150 个, 支持字符协议并发运维数≥700 个。提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能, 业务接口:千兆电口>6 个, 冗余电源。3 年产品质保;3 年软件升级。	2
40	网御星云	TD3000-FT-H-G X	国产芯片, 标准 2U 上架设备, 1 个 RJ-45 Console 口, 1 个 10/100/1000 Base-Tx 带外管理口, 4 个 10/100/1000 Base-T 接口, 4 个 SFP 光口插槽, 3 个接口扩展槽位, 2 个 USB 口, 冗余电源, 存储空间: 1T 硬盘, 32G 内存, 网络环境处理能力 (混合包、混合流): 1.5G; 最大并发连接数: 100 万, 每秒新建连接数: 2 万。提供三年软件升级 (三年 APT 静态检测服务、三年流量检测与分析服务, 三年威胁检测服务) 和原厂三年质保服务。	2
41	网御星云	leadsec-10000 WAF	2U 上架设备, 6 个 10/100/1000 Base-T 接口, 含 1 个 HA 口, 1 个 RJ-45 Console 口, 1 个 10/100 Base-Tx 带外管理口, 4 个 SFP 光口插槽, 4 个 SFP+光口插槽, 支持 4 个业	2

			务接口 bypass, 含 3 个接口永久使用授权, 2 个 USB 口, 单电源, 含应用防火墙软件一套, WAF 管理控制中心软件一套。应用层吞吐量: 20G, 最大并发 HTTP 连接数: 1000 万, 提供三年硬件保修和技术支持服务, 三年 Web 应用防护特征库升级授权	
42	网御星云	Leadsec-6000IP S-6800E	2U 上架设备, 1 个 RJ-45 Console 口, 1 个 10/100/1000 Base-T 带外管理口, 1 个 10/100/1000 Base-T HA 口, 4 个 10/100/1000 Base-T, 4 个 SFP 接口插槽, 4 个 SFP+光口插槽, 5 个网络接口扩展槽位, 2 个 USB 口, 双电源, 含嵌入式软件, 含引擎软件一套, 入侵防护系统数据中心软件一套, 提供三年硬件保修和技术支持服务, 三年应用特征库升级服务	4
43	网御星云	TAM-GUARD-G 12800N	2U 机架式软硬一体设备, 专用硬件平台和安全操作系统, 整机抗攻击能力: 10Gbps。2 个 GE 管理口, 4 个 100/1000M Base-TX 业务口, 4 个 SFP 插槽; 4 个 SFP+万兆口插槽, 4 个扩展槽, 双电源。提供三年硬件维保和技术支持服务。	2

44	H3C	SecPath M9006	1 块: 2 端口 40G 以太网光口(QSFP+,MPO) + 8 端口万兆以太网光口(SFP+,LC) + 4 端口 千兆以太网光口(SFP,LC)接口模块; 1 块: 接 口交换 A 模块(FE); 2 个: AC2500-2500W 交流电源; 1 块:下一代防火墙 D 模块; 3 块: 交换网板-B 类; 1 块: 主控制引擎模块	4
45	网御星云	Power V6000-F6510E	冗余电源;标准配置 6 个 10/100/1000M; Base-TX 接口, 4 个 SFP 接口, 具备 6 个扩 展槽位;整机吞吐量:20G, 并发连接数:420 万, 新建连接数:20 万, 支持 IPSec VPN 和 SSL VPN(免费 200 个并发用户);开通 IPS 模块, AV 模块;提供三年硬件保修和技术支持 服务, 三年 IPS、AV 应用特征库升级。配置 4 个千兆多模光模块。	2
46	H3C	S6520	24SFP Plus+2QSFP Plus+2Slot	1
47	华为	S6735-S48X6C	S6735-S48X6C(48 个万兆以太网光口, 6 个 100G 以太网光口, 双电源, 冗余风扇)	8
48	华为	S5731-S48T4X	S5731-S48T4X(48 个 10/100/1000BASE-T 以太网电口,4 个万兆 SFP+以太网光口)	4
49	H3C	S5130S	48 个 10/100/1000BASE-T 电口,4 个 1G/10G BASE-X SFP+端口; 2 个万兆多模光 模块	2

50	H3C	S6520	48 个 100/1000 BASE-X SFP 端口,支持 2 个 GE Combo 口,支持 4 个 1G/10G BASE-X SFP+端口	2
51	H3C	S9810	交换容量 43Tbps,2 个主控板,2 个交换网板,4 个 24 端口 10GE 光接口, 1800W 端口侧入风交流电源模块	2
52	H3C	S6520	48SFP Plus+2QSFP Plus+2Slot	1
53	H3C	S5560	48 个 10/100/1000BASE-T 端口,支持 4 个 10G/1G BASE-X SFP+端口,支持 1 个 Slot	1
54	H3C	S6800	4 个接口模块插槽、64 个 FC 端口、48 个光模块	2
55	H3C	S5130S	48 个 10/100/1000BASE-T 电口,4 个 1G/10G BASE-X SFP+端口	2
合 计				299

9. 其他运维服务

①乙方应根据甲方实际需求,对确需购置新设备或对旧设备更换情况,乙方须自行更换设备,必须保证系统正常运行,购置费用以采购发票为准,据实结算,采购单价不得高于同期集中采购价格,运维服务期间整体不得超过 1875000 元。

②乙方应根据甲方实际需求,按照省一朵云综合管理平

台对接标准，持续向省平台按标准推送数据。

③乙方应根据甲方实际需求，待漯河信创云服务采购完成后，按照甲方需求免费配合完成信创替代。

④为保障政务云服务的持续性，原则上乙方应依托现有机房开展运维工作，若发生机房搬迁，乙方应保证网络环境不发生变化，云平台及平台承载的业务系统不得中断，由此产生的一切费用将有乙方自行全部承担。

⑤乙方应按照甲方需求免费提供对存量宿主机以及云上 centos 操作系统进行安全加固，以满足相关部门要求。

附件 2:

漯河市 X86 政务云运维服务工作 考核评价办法（试行）

为保障全市政务信息系统安全平稳运行，确保漯河市 X86 政务云运维服务质效，在参考全国各省市政务云管理经验的基础上，依据《漯河市政务云管理暂行办法》和我市工作实际，制定本办法。

第一条 考核评价原则：

实事求是，客观公正；确保安全，保证平稳；注重规范，突出实效；标准清晰，评价全面；依据充分，简便易行。

第二条 考核评价对象：

漯河市 X86 政务云运维服务商。

第三条 考核评价频次：

考核评价周期为每一个月考核一次。

第四条 考核评价内容：

（一）合同要求和资料提供情况考核评价。该项考核评价分值为 25 分，出现以下情形扣除对应分数。

1. 市 X86 政务云服务商应按照运维服务合同要求和附件 1 服务内容提供对应的政务云运维服务，包括但不限于云平台运维服务、网络安全运维服务、网络安全资源池服务、硬件设施的运维保障服务、机房运维要求、驻场服务、故障应急响应服务等，确保 X86 政务云安全平稳运行。X86 政务云未能安全平稳运行，未造成后果。每次扣 1 分。X86 政务云

未能安全平稳运行，未造成严重后果。每次扣 3 分。

2. 市 X86 政务云服务商应按照运维服务合同要求提供对应的资料，包括但不限于《云平台配置文件》《政务云平台运维周报》《政务云巡检周报》《政务云云资源统计表》《政务云业务系统云资源利用率统计表》《云平台运维事件处理记录》《云平台信息安全事件报告单》《政务云平台故障处理报告》《政务云演练方案》《政务云演练报告》《运维服务报告》《资产信息统计表》《资产密码变更记录表》《网络结构拓扑图》《全局性访问控制策略清单》《专向性访问控制策略清单》《防护性策略清单》《权限策略清单》《安全防护策略问题整改通告单》《安全产品日常巡检记录表》《安全产品问题整改通告单》《资产安全通告》《安全产品配置策略优化单》《重大活动保障总结报告》《云租户资产对接申请单》《系统运维月度综合分析报告》《业务系统漏洞扫描季度报告》《驻场人员工作日报》《驻场人员值班表》《云平台月度运行监控月报》《机房安全管理制度》《运行维护管理办法》《安全事件管理办法》《信息安全-安全事件处理流程》《应急技术安全规范及预案》。每少提供一份资料扣 1 分。

（二）运维服务和运维管理情况考核评价。该项考核评价分值为 35 分，出现以下情形扣除对应分数。

1. 市 X86 政务云服务商应提供六人以上驻场服务，制定考勤制度和上报考勤数据，每月上报一次，市 X86 政务云主

管部门不定期抽查人员在岗情况。未上报考勤数据或每发生一次人员缺岗情况扣 5 分。

2. 市 X86 政务云服务商在收到市 X86 政务云主管部门派发的政务云资源开通通知后, 10 台以内云主机资源在 4 个小时内完成政务云资源开通, 超过 10 台的以此类推, 但总时间不超过 2 个工作日。每超时一次扣 5 分。

3. 市 X86 政务云服务商在收到市 X86 政务云主管部门派发的政务云资源变更通知后, 10 台以内云主机资源在 4 个小时内完成政务云资源变更, 超过 10 台的以此类推, 但总时间不超过 1 个工作日。每超时一次扣 5 分。

4. 市 X86 政务云服务商在收到市 X86 政务云主管部门派发的政务云资源退出通知后, 在 1 个工作日内完成政务云资源退出。每超时一次扣 5 分。

5. 市 X86 政务云服务商应提供 7×24 小时全天候技术服务, 响应时间<10 分钟。每超时一次扣 5 分。

6. 市 X86 政务云机房硬件设备上架和下架操作应征求市 X86 政务云主管部门意见, 取得同意后方可进行操作, 并在 1 个工作日内更新机房机柜落位图, 报市 X86 政务云主管部门。未按规定执行扣 5 分。

7. 市 X86 政务云设备资产台账更新后, 市 X86 政务云服务商应在 1 个工作日内报市 X86 政务云主管部门。未按规定执行扣 5 分。

8. 市 X86 政务云服务商应按照市 X86 政务云主管部门要

求，每周提供政务云运维服务情况报告。未按规定执行扣 5 分。

9. 市 X86 政务云服务商应按照市 X86 政务云主管部门要求统计政务云相关数据。未按规定执行扣 5 分。

10. 市 X86 政务云服务商应配合系统迁移。未配合扣 5 分。

11. 市 X86 政务云服务商应提供每月至少一次的政务云技术和使用培训，为市 X86 政务云主管部门工作人员讲解政务云平台的业务流程、技术架构和日常运维操作等。未按规定执行扣 5 分。

12. 市 X86 政务云服务商应按照市 X86 政务云主管部门要求进行政务云备份工作，包括但不限于硬件设备配置文件备份、政务云主要数据备份。未按规定执行扣 5 分。

13. 市 X86 政务云服务商应配合市 X86 政务云主管部门优化网络配置，如 IP 规划，并定期更新网络规划表，报市 X86 政务云主管部门。未按规定执行扣 5 分

（三）故障处置和网络安全情况考核评价。该项考核评价分值为 40 分，出现以下情形扣除对应分数。

1. X86 政务云出现故障，出现系统报错或警告，但业务系统能继续运行且性能不受影响，市 X86 政务云服务商应确保每月不超过 5 次，并在 30 分钟内提交故障处理方案，在 12 小时内修复，在 48 小时内向市 X86 政务云主管部门提交

故障分析报告。超过 5 次后每增加 1 次扣 1 分，每次超时未解决故障额外扣 2 分。

2. X86 政务云出现故障，出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作，市 X86 政务云服务商应在 30 分钟内提交故障处理方案，在 6 个小时内修复，并在 24 小时内向市 X86 政务云主管部门提交故障分析报告。每次扣 2 分，每次超时未解决故障额外扣 4 分。

3. X86 政务云出现故障，系统崩溃导致业务停止、数据丢失，市 X86 政务云服务商应在 30 分钟内提交故障处理方案，在 2 个小时内修复，并在 24 小时内向市 X86 政务云主管部门提交故障分析报告。每次扣 5 分，每次超时未解决故障额外扣 10 分。

4. 接到态势感知平台发现的安全风险通知后，政务云运维单位应 1 小时内对外部攻击 IP 进行封禁，1 天内通知具体政务信息系统运维单位进行漏洞修复。每出现一次逾期未处理，扣除 5 分；逾期未处理造成外部攻击成功或主机失陷、数据泄露的，额外扣除 30 分，同时按相关要求，移交相关部门追究责任。

5. 因市 X86 政务云原因受到市网信办或网警网络安全通报，每次扣 2 分。

6. 因市 X86 政务云原因受到省网信办或网警网络安全通报，每次扣 10 分。

7. 因市 X86 政务云原因受到国家网信办或网警网络安全通报，每次扣 20 分。

（四）一票否决项

1. 市 X86 政务云服务商应按照运维服务合同要求和附件 1 服务内容提供对应的政务云运维服务，包括但不限于云平台运维服务、网络安全运维服务、网络安全资源池服务、硬件设施的运维保障服务、机房运维要求、驻场服务等，确保政务云安全平稳运行。政务云未能安全平稳运行，造成严重后果（包括但不限于因市 X86 政务云原因导致业务系统掉线造成重大负面影响、因市 X86 政务云原因受到市委市政府通报批评、因市 X86 政务云原因导致数据泄露、因市 X86 政务云原因导致安全事故、因市 X86 政务云原因收到投诉或举报造成重大负面影响等），直接扣除当月费用。

2. 若出现材料或上报情况造假，直接扣除当月费用。

第五条 考核结果评定：

每次考核评价总分为 100 分，按照本办法第四条的考核评价内容逐项评定得分，各分项评分相加为最终得分。

得分 90 分以上，当月考核评定等级为优秀，全额认定当月运维费用；

得分 80-89 分，当月考核评定等级为良好，合同执行期间首次评定为良好档次，乙方需及时整改，整改情况及时报送至市 X86 政务云主管部门，主管部门按程序审核通过后，

全额认定当月运维费用。以后评定为良好档次，扣除当月运维费用的 5%；

得分 70-79 分，当月考核评定等级为一般，扣除当月运维费用的 10%，乙方出具问题分析报告及整改报告；

得分 60-69 分，当月考核评定等级为较差，扣除当月运维费用的 20%，乙方出具问题分析报告及整改报告；

得分不足 60 分，当月考核评定等级为差，直接扣除当月费用，乙方出具问题分析报告及整改报告。