登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目合同

项目名称：登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目

项目内容：第二标段：安全设备

合同编号：登工招 202512166

甲　　方：登封市行政审批和政务信息管理局

乙　　方：中国移动通信集团河南有限公司郑州分公司

签订时间：2026年 2 月 27 日

第一节 合同协议书

甲方（招标人）：登封市行政审批和政务信息管理局

乙方（投标人）：中国移动通信集团河南有限公司郑州分公司

依据《中华人民共和国民法典》等有关的法律法规，以及本招标项目**甲方的《招标文件》**、乙方的《投标文件》及《中标通知书》，甲方、乙方同意签订本合同。具体情况及要求如下：

一、项目信息

（1）项目名称：登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目 第二标段：安全设备

项目编号：登工招202512166

（2）采购计划编号：登工招202512166

（3）项目内容：

① 乙方在现有技术条件下、现有网络覆盖范围内，为甲方有偿提供【登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目 第二标段：安全设备】项目硬件设备销售，以及对应的设备安装、系统集成、质保服务。

② 乙方为甲方提供的具体服务内容、价格、技术参数及相关要求详见【附件1：设备清单及技术规范】。当附件与合同正文不一致时，以合同正文为准，但涉及技术规范等专业性内容以附件中更为详细、准确的规定为准，前提是附件内容不与合同基本宗旨冲突，如实际执行中双方根据业务需求有更细化深化的技术方案，则以双方书面确认的材料为准。

（4）政府采购组织形式：☐ 政府集中采购 ☐ 部门集中采购 ☑ 分散采购

（5）政府采购方式：☑ 公开招标 ☐ 邀请招标 ☐ 竞争性谈判 ☐ 竞争性磋商

☐ 询价 ☐ 单一来源 ☐ 框架协议 ☐ 其他：/

（6） 中标采购标的制造商是否为中小企业：☐ 是 ☑ 否

中标（成交）采购标的制造商是否为残疾人福利性单位：☐ 是 ☑ 否

中标（成交）采购标的制造商是否为监狱企业：☐ 是　　☑ 否

（7）合同是否分包：☐ 是　　☑ 否

（8）中标（成交）投标人是否为外商投资企业：☐ 是　　☑ 否

外商投资企业类型：☐ 全部由外国投资者投资　☐ 部分由外国投资者投资

（9）是否涉及进口产品：☐ 是☑ 否

（10）是否涉及节能产品：

☑ 是，《节能产品政府采购品目清单》的底级品目名称：___/___

☐ 强制采购　　☑ 优先采购　　☐ 否

是否涉及环境标志产品：

☑ 是，《环境标志产品政府采购品目清单》的底级品目名称：___/___

☐ 强制采购　　☑ 优先采购　　☐ 否

是否涉及绿色产品：

☐ 是，绿色产品政府采购相关政策确定的底级品目名称：___/___

☐ 强制采购　　☐ 优先采购　　☑ 否

（11）涉及商品包装和快递包装的，是否参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》明确产品及相关快递服务的具体包装要求：☑ 是 ☐ 否　　☐ 不涉及

二. 合同金额

2.1 本合同项下甲方应当向乙方支付的合同款项（含税）共计小写：3766600.00 元 大写：叁佰柒拾陆万陆仟陆佰圆整，费用对应的明细清单详见【附件2：费用明细表】。

2.2 合同定价方式（采用组合定价方式的，可以勾选多项）：

☑ 固定总价 ☐ 固定单价 ☐ 固定费率 ☐ 成本补偿 ☐ 绩效激励 ☐ 其他___/___

2.3 付款方式（按项目实际勾选填写）：

☐全额付款：_____/_____

☑ 分期付款：合同签订后付合同款的30%，完成合同50%工程量(工程量见附件1内容)后付到合同款的50%，完成合同80%工程量(工程量见附件1内容)后付到合同款的80%，项目完工验收合格后付到合同款的95%，剩余5%竣工审计结算后付清。财政资金拨付到甲方单位银行账户后，甲方在20个工作日内以人民币转账方式支付至乙方指定的银行账户

□成本补偿：/ （应明确按照成本补偿方式的支付方式和支付条件）

□绩效激励：/ （应明确按照绩效激励方式的支付方式和支付条件）

2.4 双方银行账户信息

甲方名称：【登封市行政审批和政务信息管理局】

纳税人识别号：【11410185MB1679588K】

户名：【登封市行政审批和政务信息管理局】

开户行：【 】

账号：【 】

地址：【河南省登封市少林大道东段136号】

联系电话：【0371-62826089】

乙方名称：【中国移动通信集团河南有限公司郑州分公司】

纳税人识别号：【914101007167688597】

户名：【中国移动通信集团河南有限公司郑州分公司】

开户行：【中国银行股份有限公司郑州花园支行】

账号：【252061053060】

地址：【郑州市金水区北环路 11 号1号楼】

联系电话：【13598890012 】

任何一方如需改变上述账户信息信息（名称和纳税人识别号不可改变），应在变更账户前十（10）日以书面通知另一方并征得对方同意。如一方未按本合同约定单独变更账户信息而使另一方遭受损失的，应予以赔偿。

2.5 结算周期内甲方向乙方支付的费用为：结算金额＝Σ（应付合同金额±违约金）（说明：如甲方违约则使用“＋”，若乙方违约则使用“－”）。

2.6 结算方式采用【转账】的形式。

2.7 在甲方支付本合同项下的服务费之前，乙方应当向甲方开具相应金额的增值税【普通】（普通/专用）发票，财政资金拨付到甲方单位银行账户后，甲方在20个工作日内以人民币转账方式支付至乙方指定的银行账户。**如财政资金未按时拨付，导致甲方不能按约定付款的，甲方不构成违约。**

2.8 合同履行过程中，如遇国家税率政策变更，对于合同未履行完毕的部分，在原标的不含税（单）价不变的基础上，按照新税率重新计算标的含税（单）价或合同总价，并且继续履行。

三. 合同履行

3.1 乙方应在收到甲方书面通知之日起【360】日内完成平台及硬件集成及调试，达到交付验收标准。

3.2 自项目验收通过之日起提供质保服务，质保期为【5】年。若因甲方需求变更、未能及时提供必要的资料、数据、授权或测试环境等甲方原因导致项目未能验收，本项目质保期自乙方提交验收申请7个工作日起开始计算。

3.3 履约地点：登封市行政审批和政务信息管理局

3.4 履约担保：是否收取履约保证金：☐ 是 ☑否

收取履约保证金形式： /

收取履约保证金金额： /

履约担保期限： /

3.5 分期履行要求： /

3.6 风险处置措施和替代方案： /

四. 合同验收

4.1 设备验收

4.1.1甲方指定的地点及收货人：登封市行政审批和政务信息管理局 【赵彬朴】。

4.1.2开箱检验在乙方将货物运送至甲方指定交货地点后【2】日内进行，双方根据合同约定检查货物，检验后无任何问题的签署开箱检验合格证书。

4.1.3其他：/。

4.2 集成验收

4.2.1本项目验收标准详见【附件3：项目验收标准】。如未约定或约定不明确的，按照中华人民共和国国家和履约地相关质量标准、行业技术规范标准执行。

4.2.2 在乙方完成集成服务【7】个工作日内，甲方和乙方结合项目验收标准成立验收小组（建设单位、承建单位、监理单位、使用单位）对项目成果进行验收，各项功能及指标（技术、服务、货物规格、质量要求、安全标准、试运行）符合招投标文件要求的，验收小组成员单位签署项目验收合格报告。

五. 组成合同的文件

5.1本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释：

（1）招标文件

（2）合同协议书及其变更、补充协议

（3）合同专用条款

（4）合同通用条款

（5）中标通知书

（6）投标文件

（7）有关技术文件，图纸

（8）国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件

5.2 本项目质保服务5年，在质保期间系统免费升级维护并配合采购人平台运营工作，规范详见【附件4：质保服务规范】。

5.2.1 硬件设备发生损坏的，若在质保期内，设备维修或更换的成本由乙方承担（因甲方故意或使用不当导致设备损坏的除外）；若在质保期外，设备维修或更换的成本由甲方承担。

5.2.2其他：_____/_____。

六　甲方的权利和义务

6.1在本合同有效期内，甲方有权要求乙方根据本合同约定和产品使用说明的描述向甲方提供相应的产品和服务。

6.2甲方同意乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

6.3甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

6.4甲方承诺并保证不利用乙方提供的设备或服务进行任何违反国家政策法律法规、侵犯乙方或第三方合法权利的行为，否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。

6.5 甲方如对乙方提供的产品和服务的费用产生异议，须于乙方向甲方通知相关费用之日起【15】日内向乙方提出，否则视为对费用的认可。

6.6 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

6.7 甲方使用乙方提供的本合同约定产品或服务时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品或服务的，相关责任由甲方承担。

6.8 甲方成为乙方集团客户后，如果乙方提供了服务账号，甲方应妥善保管乙方提供的相关服务账号和甲方设定的服务密码。服务账号和密码是甲方办理产品相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。

6.9 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将产品或服务提供给甲方，甲方承担由此造成的责任和后果。

6.10 该项目内容的全部知识产权（包括但不限于著作仅、专利申请权等）自初验后起，完全归属于甲方。乙方未经甲方书面同意，不得以任何方式向第三方披露、转让和许可有关的技术成果、计算机软件、技术诀窍、秘密信息、技术资料和文件。

6.11 其他：/。

七、乙方的权利和义务

7.1乙方应按合同约定向甲方提供相关硬件设备，并完成系统集成、维护等工作。乙方人员应携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

7.2乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定产品或服务的，应提前通知甲方，甲方应给予必要的配合。

7.3乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

7.4在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

7.5 因第三方实施破坏、网络攻击等非乙方原因导致甲方不能正常使用乙方产品和服务的，乙方应于配合，及时处理相关问题，使问题妥善解决。

7.6乙方应对其所委托的代为向甲方提供本合同项下服务的第三方的服务行为向甲方承担责任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

7.7乙方应严格履行《登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目招标文件》第四章采购需求要求。

7.8其他：无。

八、 保密条款

8.1"保密信息"是指本协议拥有信息的一方（"提供方"）根据本协议向另一方（"接受方"）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于：技术方案、客户数据、技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

8.2保密信息只能由接受方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。甲方理解并同意，乙方及其关联公司可通过业务受理系统登记、纸质档案，通过网络接收、读取并记录等方式，以提供电信服务为目的，在业务活动中收集、使用甲方提供的和甲方使用服务过程中形成的信息。乙方

有权依法对包含甲方在内的整体用户数据进行分析并加以利用，包括不限于匿名化处理后的统计分析等。未经甲方同意，乙方不向除乙方关联公司外的第三方提供甲方信息。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

8.3双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；双方承诺采取不低于国家标准的技术措施保护数据安全，不得将数据存储于境外，禁止数据跨境传输，同时，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

8.4接受方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接受方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。接受方应向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

8.5如相关政府部门或监管机构要求接受方披露任何保密信息，接受方可在该政府部门或机构要求的范围内做出披露而无需承担本协议项下的保密责任。但前提是，该接受方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接受方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。

8.6双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性及对甲乙双方的约束力。

8.7由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

8.8在任何情形下，本合同约定的保密义务应永久持续有效。

九、 数据安全与保护

9.1 本条款所称“数据”是指双方在履行本合同过程中，由甲方提供或授权乙方处理、以及乙方在提供服务过程中产生的所有电子数据。

9.2 双方承诺严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规及国家标准，履行数据安全保护义务。

9.3甲方应保证其向乙方提供、授权乙方处理的所有数据来源合法，已获得必要的授权和同意，并具备允许乙方为实现本合同目的而处理该等数据的完整权利。

9.4如甲方对数据的处理有特殊的安全要求，应在附件或另行书面签署的协议中明确告知乙方，双方协商一致后共同执行。

9.5乙方将采取符合业界标准的安全技术措施（如加密传输、访问控制等）来保护数据的安全性与机密性，甲方应协助乙方防止数据泄露、毁损、丢失、未经授权的访问、使用或披露。

9.6本合同终止或提前解除后，乙方应根据甲方的书面要求，及时返还或在本协议约定的合理期限内安全删除其持有的一切相关数据（法律法规另有规定的除外）。

9.7 本项目涉及的建设内容全部按纯国产化建设和采购，同时按上级文件精神后期做好国产化免费升级工作。

9.8 如甲方违反本条款约定，乙方有权停止提供所涉服务并解除合同，因此造成的责任和后果由甲方承担。

十、违约责任

10.1甲方未按照本合同约定（财政资金拨付到甲方单位银行账户后，甲方在20个工作日内以人民币转账方式支付至乙方指定的银行账户）的期限支付合同款项的，从逾期的次日起计算违约金，每滞后1天支付合同未付金额的【0.3‰】的违约金。

10.2因乙方原因导致乙方未按照本合同约定时间完成项目的，每逾期一天甲方应扣除未完成服务对应合同金额0.3‰的违约金。乙方在进行网络调整和维护时需要短时间中断服务，或者由于Internet上骨干网通路的阻塞造成甲方服务器访问速度下降，甲方认同属于正常情况，不视为乙方违约。

10.3下列情况下乙方有权单方终止本合同，并停止向甲方提供服务。由此给甲方造成的损失，乙方不承担责任，并有权要求甲方承担违约或赔偿责任：

（1）甲方（包括联系人）提供虚假证照的；

（2）甲方利用乙方提供的产品和服务实施违反国家法律、法规和政策的；

（3）甲方利用乙方提供的产品和服务从事其他不当用途（如：甲方将乙方提供用于本合同业务的相关设备转售、转租、转借第三方，或将乙方提供的设备、产品和服务接入其他通信服务提供商的业务）或侵犯第三方的合法权利；

（4）乙方根据国家有关部门的要求停止为甲方提供相关服务；

（5）甲方所使用的所有产品和服务中有一项产品欠费超过三个月，或有二项以上产品欠费均超过一个月。

10.4 乙方应对因其过错给甲方造成的直接损害结果（如修复费用、合理停机损失）承担赔偿责任。

10.5 其他：无。

十一、不可抗力及免责条款

11.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

11.2 由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：（1）受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)天内提供有关该事件的书面说明，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。

11.3 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。受阻方应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。

11.4 如果不可抗力事件的影响持续达三十（30）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。

11.5 因乙方难以避免、难以排除的技术或网络故障或第三方原因造成甲方无法使用本协议项下服务的，乙方应尽合理努力争取在最短时间内解决。鉴于计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断，进出口管制、关税等国际贸易政策变化等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方认同不属于乙方违约。

十二、通知与送达

12.1根据本合同需要发出的全部通知，均须采取书面形式，对本合同效力产生影响的、或解决合同争议时的通知或函件，必须采用专人递送或者特快专递方式送达，上述书面通知均须标明合同对方为收件人。

12.2上述书面通知按对方在本合同通知与送达条款中所列的地址发出，任何一方未按照本合同约定的送达方式送达的，视为未履行通知送达义务。如双方中任何一方的地址有变更时，须在变更前十日以书面形式通知对方。因一方在本合同所列的地址错误或变更地址未通知导致另一方文件未送达的，视为已送达。

12.3双方将按如下约定确定通知送达完成时间：

12.4 以专人递送的，接收人签收之日视为送达；

12.5 以特快专递形式发出的，发往本市内的，发出后第【3】日视为送达。发往国内其他地区的，发出后第【5】日视为送达；

12.6 以电子邮箱形式发出的，到达接收人电子邮箱所在系统之时视为送达；

同时采用上述两种或两种以上方式的，以其中最快达到对方者为准。

12.7合同各方均明知：因各方提供或者确认的通信地址和联系方式不准确、 或者通信地址变更后未及时依程序告知对方和司法机关、或者当事人和指定接收人拒绝签收等原因，导致商业信函、诉讼文书等未能被当事人实际接收，以专人递送的，送达至本条款约定的地址之日即视为送达之日，送达人可采取拍照、录像方式记录送达过程，并将文书留置；以特快专递形式发出的，按照本条款约定的时间确定送达之日。

12.8各方地址与联系方式如下：

甲方：【登封市行政审批和政务信息管理局】

地址：【登封市少林路东段 】

电话：【0371-62826089】

联系人：【赵彬朴】

乙方：【中国移动通信集团河南有限公司郑州分公司】

地址：【郑州市金水区北环路 11 号1号楼】

电话：【13598890012】

联系人：【杜洪飞】

十三、争议解决

13.1本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

13.2如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。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。

13.3如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则双方同意向甲方住所地人民法院提起诉讼。

13.4诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。本合同全部或部分无效的，争议解决条款依然有效。

十四、 合同生效

本合同自_____签订之日起_____生效。

十五、合同份数和其他约定

15.1本合同一式【陆】份，甲方持【肆】份，乙方持【贰】份，具有同等法律效力。

15.2 对于合同未尽事宜，双方可签订补充合同做出补充、说明、解释。

15.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

15.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除。任何一方欲变更或解除本协议，应提前30日向另一方提交书面说明，经各方协商一致后，以书面形式进行变更或解除。除合同约定的情形外，未经双方同意不得单方进行变更或解除协议，违约方应对另一方因此遭受的损失承担全部赔偿责任。

15.5 本协议自双方法定代表人（负责人）或授权代表签字并加盖公司印章之日起生效；如双方签署日期不一致，自较迟的签署日起生效。

十六. 本合同附件

附件1：设备清单及技术规范

附件2：费用明细表

附件3：项目验收标准

附件4：质保服务规范

附件5：网络与信息安全承诺书

合同订立时间：2026 年 2 月 27 日

合同订立地点：登封市行政审批和政务信息管理局

甲方（投标人）		乙方（投标人）	
单位名称（公章）	法定代表人或其委托代理人（签章）	单位名称（公章）	法定代表人或其委托代理人（签章）
甲方联系人	赵彬朴	乙方联系人	杜洪飞
甲方联系电话	0371-62826089	乙方联系电话	13526881669
甲方通信地址	登封市行政审批和政务服务管理局	乙方通信地址	郑州市金水区北环路11 号1号楼
甲方邮政编码		乙方邮政编码	450000
甲方电子邮箱		乙方电子邮箱	
甲方统一社会信用代码		乙方统一社会信用代码	914101007167688597
甲方开户名称		乙方开户名称	中国移动通信集团河南有限公司郑州分公司
甲方开户银行		乙方开户银行	中国工商银行股份有限公司郑州行政区支行
甲方银行账号		乙方银行账号	1702029109201027859

……（以下无正文）

附件1：设备清单及技术规范

安全设备					
序号	设备及软件名称	主要性能指标	数量	单位	备注
—	本地机房安全				
1	终端威胁检测与响应系统（EDR）	含服务端管理控制台的授权许可，包含客户端基础功能：资产管理、运维管理、病毒查杀、外设管理、非法外联监控、网络管理、终端响应、日志管理等基础功能；提供50个点位授权；提供5年客户端及规则库升级、病毒库升级授权服务。	1	套	办公区
2	网络接入控制系统（NAC）	标准2U设备，冗余电源，国产化CPU和操作系统；网络接口：提供千兆电口≥6个，千兆光口≥4个，扩展槽位≥2个；硬盘≥SSD 500G；内存≥8G；最大支持终端数≥1000；提供终端准入授权≥50点（含终端安全检查授权），提供5年硬件质保服务。	1	台	办公区
3	Web应用防火墙系统（WAF）	标准1U设备，冗余电源，国产化CPU和操作系统，网络接口：提供千兆电口≥6个、千兆光口≥4个，1个管理接口，1个HA口，扩展插槽≥2个，内存≥16G，硬盘≥500G SSD；HTTP吞吐量≥2Gbps，最大并发HTTP连接数≥150万，每秒新建HTTP连接数≥4万个，每秒新建HTTP事务数≥5万。提供5年Web特征库升级服务， 提供5年硬件质保服务。	2	台	登封联通机房 互联网区和政务外网区各1台
4	漏洞扫描系统	标准1U设备，冗余电源，国产化CPU和操作系统；网络接口：提供千兆电口≥6个、千兆光口≥4个，接口扩展插槽≥2个，硬盘≥500GB SSD + 8TB SATA，内存≥16G；开通主机漏扫、配置核查、Web漏扫功能；主机漏扫和基线核查可扫描IP地址总数无限制，单任务最大可扫描100IP地址；主机漏扫并发扫描100IP地址，基线核查可核查Windows系列设备类型，Web漏扫可扫描子域名或IP总数量为5个，Web漏扫并发为5个子域名或IP； 提供主机漏扫、配置核查、Web漏扫3个模块5年漏洞库升级服务，提供5年硬件质保服务。	1	台	登封联通机房 电子政务外网区
5	数据库审计系统	标准1U设备，冗余电源，国产化CPU和操作系统；网路接口：提供千兆电口≥4个，千兆光口≥4个，1个带外管理口，1个HA口，扩展槽位≥3个；硬盘≥8T；内存≥16G；可审计流量≥300Mbps；每秒入库速度≥15000条/秒。提供13个DB服务数授权。提供5年硬件质保服务。	1	台	登封联通机房 电子政务外网区
6	SSL VPN网关	标准2U设备，冗余电源，国产化CPU和操作系统，内置加密卡；网络接口：提供千兆电口≥	2	台	登封联通机房

安全设备					
序号	设备及软件名称	主要性能指标	数量	单位	备注
		8个、千兆光口≥4个，扩展槽≥2个；内存≥16G；系统存储≥mSATA 1T；整机吞吐量≥8Gbps，SSL VPN加密速度≥400Mbps，SSL VPN最大并发用户数≥2000；IPSec VPN加密速度≥400Mbps；IPSec VPN最大隧道数≥8000；			
		提供50个SSL VPN并发用户授权，支持PC和移动接入，提供5年硬件质保服务。			互联网区和政务外网区各1台
7	运维安全网关系统（堡垒机）	标准1U设备，冗余电源，国产化CPU和操作系统；网络接口：提供千兆电口≥6个、千兆光口≥4个，扩展槽≥3个；字符并发≥800，图形并发≥200；内存≥16G，有效存储≥8T；	1	台	登封联通机房
		实配管理授权数：50个，提供5年硬件质保服务。			互联网区
8	安全管理系统（日志审计）	标准1U设备，冗余电源，国产化CPU和操作系统；网络接口：提供千兆电口≥6个、千兆光口≥4个，扩展槽≥3个；内存≥16G，系统盘≥1T SSD，有效存储≥8T；日志处理性能≥ 3000EPS；实配50个审计授权。	1	台	登封联通机房
		提供30个管理对象授权，授权永久有效；提供5年硬件质保服务。			互联网区
二	云上安全				
1	Web应用防火墙系统（WAF）	基于对HTTP及HTTPS流量内容的双向检测分析，为Web应用提供实时的防护；支持SQL注入、XSS攻击、网页木马、WEBSHELL等Web威胁防护；支持8核引擎。	4	套	政务云专有云和公有云各1套*2个机房
		提供5年Web特征库升级服务。			
2	网站安全监测服务	提供8个域名5年的网站安全监测服务。	1	套	SaaS服务
		监测项目包括：网站漏洞扫描、挂马监测、可用性监测、页面篡改监测、域名解析监测、敏感内容监测，黑词黑链检测。通过网站安全监测平台对网站进行自动化监测，通过邮件、短信进行及时报警，每周、每月发送监测报告。默认支持添加3个手机号接收短信告警。			
		安全通告服务：收集和整理安全漏洞、安全事件、安全资讯等信息，定期发送给客户，使客户了解当前互联网风险趋势，及时采取应对措施，降低风险，减少损失。报告频率：每周1次。			
3	漏洞扫描系统	开通主机漏扫、配置核查、Web漏扫功能。	2	套	政务云专有云1套*2个机房
		主机漏扫和基线核查可扫描IP地址总数无限制，单任务最大可扫描100IP地址：主机漏扫并发扫描100IP地址：基线核查可核查Windows系列设备类型；Web漏扫可扫描子域名或IP总数量为5个，Web漏扫并发为8个子域名或IP.			

		提供主机漏扫、配置核查、Web漏扫3个模块5年漏洞库升级服务。			
4	安全管理系统（日志审计）	提供主机操作系统、网络设备、安全设备日志收集，查询，告警，审计，报表等功能。 提供50个审计对象授权，5年软件升级服务.	4	套	政务云专有云和公有云各1套*2个机房
5	终端威胁检测与响应系统（EDR）	含服务端管理控制台的授权许可，包含客户端基础功能：资产管理、运维管理、病毒查杀、外设管理、非法外联监控、网络管理、终端响应、日志管理等基础功能； 提供100个点位授权； 提供5年客户端及规则库升级、病毒库升级授权服务。	4	套	政务云专有云和公有云各1套*2个机房
6	API接口监测系统	围绕业务API接口，采用实时监测技术，对API接口数据进行协议解析，对接口数据流转环节进行风险关联分析，实现敏感数据传输与违规监测、异常行为风险监测，以确保日常数据处理活动的安全、合规；提供5年软件升级服务。	2	套	政务云专有云1套*2个机房
7	数据库审计系统	针对业务环境下的数据库操作行为进行细粒度审计。通过对被授权人员和系统的网络行为进行解析、分析、记录、汇报，以帮助用户事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源，加强内外部网络访问行为监管。 提供13个DB服务数授权 和 13个虚拟导流器功能授权，5年软件升级服务；	2	套	政务云专有云1套*2个机房
三	本地密码安全设备				
1	云服务器密码机	标准2U机架设备，冗余电源，国产化CPU和操作系统，内置加密卡，具备1块显示屏，支持液晶屏显示设备网络信息、CPU占用、网关信息、当前系统虚机数量及运行状态等信息；网络接口：提供千兆电口≥8个，SFP插槽≥4个 ， 扩展插槽≥2个，内存≥64G，固态硬盘≥8T， 并发连接≥31000，SM4算法加解密速度≥7000Mbps；产品需具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书 》，为保障安全体系建设的安全合规，设备厂商所提供的设备需是在省级保密部门备案过的设备，提供5年硬件质保服务。	3	台	政务外网区1台*3个机房
2	签名验签服务器	标准2U机架设备，冗余电源，国产化CPU和操作系统，内置加密卡；网络接口：提供千兆电口≥8个，SFP插槽≥4个，扩展插槽≥2个，内存≥16G，硬盘≥8T；最大并发连接≥12000，SM2 PKCS1签名/验签速率（次/秒）≥90000/60000，SM2 PKCS7签名/验签速率（次/秒）≥70000/52000，提供5年硬件质保服务。	3	台	政务外网区1台*3个机房
		标准2U设备，冗余电源，国产化CPU和操作系统，内置加密卡；网络接口：提供千兆电口≥8个、千兆光口≥4个，扩展槽≥2个；内存≥8G			政务云专有云和公有云各1台*2个机房；

3	SSL VPN网关	：系统存储≥mSATA 1T；整机吞吐量≥8Gbps，SSL VPN加密速度≥400Mbps，SSL VPN最大并发用户数≥2000；IPSec VPN加密速度≥400Mbps；IPSec VPN最大隧道数≥8000；提供50个SSL VPN并发用户授权，支持PC和移动接入，提供5年硬件质保服务。	4	台	登封本地机房的SSLVPN在等保清单已列；
4	IPSec VPN网关	标准2U设备，冗余电源；千兆电口≥6个，千兆光口≥4个，扩展槽≥2个；CPU：兆芯C4710,2.0GHz,4核；内存≥4G；系统存储≥mSATA 500G；操作系统：中标麒麟V7.0；内置加密卡；整机吞吐量≥1.8Gbps，IPSec VPN加密速度≥240Mbps，IPSec VPN最大隧道数≥ 5000；提供3年硬件质保服务。	3	台	政务外网区1台*3个机房
5	智能密码钥匙	实现数字证书的安全存储与使用； 标准USB2.0规范，兼容USB1.1，兼容3.0规范接口； 提供标准安全中间件 CSP 及 PKCS#11 v2.11接口，硬件实现数字签名，支持X.509 v3标准证书格式； 支持Windows2000/2003/2008/XP/Vista/Win7/Win8等32位和64位中文、英文、繁体操作系统； 支持1024/2048位RSA和SM2非对称算法，支持SSF33、SM1、SM3、SM4等国密算法。	66	个	50个办公终端+12台VPN（4台*3机房）+4个密码管理员（自签证书，含1个租户管理员）
6	个人数字证书	由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循X.509 V3格式标准；	150	个·年	50终端*5年服务
7	设备数字证书	由权威合法的第三方CA机构签发，符合《x.509C的国内数字证书格式规范》。证书标准遵循X.509 V3格式标准；	27	个·年	9台VPN*5年服务
8	国密浏览器	1、支持SM2、SM3、SM4国密算法； 2、支持国密SSL双向协议； 3、支持最新TLCP标准； 4、支持沙箱机制、浏览器内核隔离域、跨域安全隔离、站点安全隔离防护、可信证书校验等功能； 5、支持本地用户数据加密，防止用户保存的密码被明文导出； 6、支持国密网站、国密应用自动识别及国密标识展现，针对国密网站优先通过国密协议访问。	5	个	5个办公终端使用
9	国密OV SSL证书（通配型）	标识网站真实身份，能够实现网站身份验证，能有效防范假冒网站和钓鱼网站，它同时也是信息的传输通道加密，确保数据加密传输和数据完整性。	6	个·年	2个公众网站*5年

附件2：费用明细表

项目名称	合同内容	未含税总价（元）	税率（%）	增值税税额（元）	含税总价（元）
登封市城市大脑-智慧城市建设项目（二期）-智慧农业、安全设备建设项目（第二标段）	设备费	1646017.70	13	213982.30	1860000
	安全系统服务费	1396226.42	6	83773.58	1480000
	系统集成费	336415.09	6	20184.91	356600
	安装服务费	36697.25	9	3302.75	40000
	维保费	28301.89	6	1698.11	30000
合计		3443658.34	/	322941.66	3766600

附件3：项目验收标准

1 总则

1.1 验收目的

本标准旨在规范网络安全设备系统集成项目（以下简称“本项目”）的验收流程与要求，全面检验项目成果是否符合合同约定、技术规范及相关国家标准，确保项目建成后能够稳定、可靠、安全地运行，满足建设单位的网络安全防护需求。

1.2 验收依据

项目相关合同及附件（含技术协议、补充协议等）；

国家及行业相关标准规范，包括但不限于《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）、《信息安全技术 信息系统安全集成实施指南》（GB/T 25070）、《计算机信息系统安全保护等级划分准则》（GB 17859）等；

项目需求规格说明书、系统设计方案、实施方案、测试报告等项目过程文档；

设备厂商提供的产品技术手册、质量合格证明等相关资料。

1.3 验收范围

本标准覆盖本项目所涉及的全部网络安全设备、系统软件、集成服务及相关文档资料，具体包括：

网络安全硬件设备：防火墙、入侵检测/防御系统（IDS/IPS）、VPN设备、Web应用防火墙（WAF）、安全审计系统、终端安全管理设备、数据防泄漏设备等；

安全软件及系统：操作系统、数据库系统、安全管理平台、漏洞扫描软件等；

集成服务成果：设备部署与调试、系统联调、网络安全策略配置、数据迁移与备份、系统优化等；

项目相关文档：需求分析报告、设计方案、实施报告、测试报告、用户手册等。

1.4 验收原则

合规性原则：验收过程及结果需符合合同约定、国家及行业相关标准规范；

客观性原则：以实测数据、测试报告及相关文档为依据，客观公正地评价项目成果；

完整性原则：全面覆盖验收范围，确保所有项目成果均通过检验；

实用性原则：验收标准需结合项目实际应用场景，确保系统建成后能够满足建设单位实际需求；

安全性原则：重点检验系统的安全防护能力，确保系统具备抵御常见网络攻击的能力，保障数据安全与业务连续性。

2 验收基本要求

2.1 项目完成度要求

所有合同约定的网络安全设备已全部到货、安装部署完毕，并通过通电测试；

所有安全软件及系统已成功安装、配置完成，能够正常启动并运行；

系统集成工作已全部完成，包括设备间的互联互通、安全策略的部署与验证、与原有网络系统的无缝对接等；

合同约定的其他服务内容（如人员培训、技术支持等）已全部履行完毕。

2.2 设备及软件质量要求

网络安全设备需具备产品质量合格证明、3C认证（如适用）等相关资质文件，设备型号、规格、参数需与合同约定一致；

设备及软件运行稳定，无硬件故障、软件崩溃、死锁等异常情况。

2.3 系统集成功能验收

设备互联互通：所有网络安全设备之间、网络安全设备与原有网络设备之间能够正常通信，数据传输顺畅，无丢包、延迟过高现象；

安全策略协同：各安全设备的安全策略配置合理、协同有效，形成完整的网络安全防护体系，无策略冲突、策略漏洞等问题；

与原有系统对接：项目建成的网络安全系统能够与建设单位原有业务系统、管理系统无缝对接，不影响原有系统的正常运行；

数据迁移与备份：若涉及数据迁移，迁移后的数据完整、准确，无丢失、损坏或不一致现象；数据备份功能正常，能够按约定的备份策略完成数据备份，备份数据可正常恢复；

2.4 安全性能及稳定性验收

性能测试：系统在设计的最大负载（如最大并发用户数、最大数据吞吐量等）情况下，各项性能指标（如响应时间、处理能力、资源利用率等）需符合合同约定；

稳定性测试：系统连续无故障运行时间需符合合同约定（建议不低于72小时），运行期间无硬件故障、软件崩溃、功能异常等情况；

压力测试：在超过设计负载的情况下，系统能够通过合理的方式进行处理（如限流、告警等），不出现严重故障或数据丢失；

安全渗透测试：由专业安全测试机构或人员进行渗透测试，系统需能够抵御常见的渗透攻击，无高危安全漏洞；

灾难恢复测试：模拟系统故障或灾难场景（如设备故障、网络中断、数据损坏等），系统能够按照应急处理预案完成灾难恢复，恢复时间（RTO）、恢复点（RPO）符合合同约定。

2.5 人员培训及技术支持验收

培训内容：培训内容需覆盖系统的安装、配置、操作、维护、故障排查等核心内容，符合培训计划要求；

培训效果：建设单位相关运维人员能够熟练掌握系统的基本操作及日常维护技能，能够独立处理常见故障；

技术支持：项目实施方需提供合同约定的技术支持服务，包括现场支持、远程支持、电话支持等，响应时间及解决问题能力符合合同要求；

售后服务承诺：项目实施方需提供明确的售后服务承诺，包括质保期、质保范围、售后服务流程等，符合合同约定。

2.6 整体质量验收标准

项目整体质量达到“合格”标准，符合国家及行业内有关标准及规定；

建设期控制在 360 日历天内，无逾期竣工情况。

附件4：质保服务规范

（一）质保期限

本项目整体质保期限为5年，自项目验收合格之日起计算；若因甲方需求变更、未能及时提供必要的资料、数据、授权或测试环境等甲方原因导致项目未能验收，本项目质保期自乙方提交验收申请7个工作日起开始计算。质保期间软件免费升级维护并配合甲方进行平台运营工作。

（二）质保范围

1. 硬件设备质保范围

本项目合同约定的所有网络安全硬件设备，包括但不限于防火墙、入侵检测/防御系统（IDS/IPS）、VPN设备、Web应用防火墙（WAF）、安全审计系统、终端安全管理设备、数据防泄漏设备等。质保范围涵盖设备本身的质量问题，包括硬件故障、性能下降、接口损坏等（非人为损坏、自然灾害等不可抗力因素除外）。

2. 软件及系统质保范围

本项目合同约定的所有安全软件及系统，包括操作系统、数据库系统、安全管理平台、漏洞扫描软件等。质保范围涵盖软件本身的功能缺陷、运行异常、兼容性问题等，乙方需提供软件补丁更新、版本升级（若合同约定包含）等服务（因甲方违规操作、第三方软件干扰等导致的问题除外）。

3. 集成服务质保范围

本项目实施的系统集成服务成果，包括设备部署与调试、系统联调、安全策略配置、数据迁移与备份、系统优化等。质保范围涵盖集成服务过程中出现的配置错误、策略冲突、系统对接异常等问题，乙方需及时排查并解决，确保集成功能正常实现（因甲方业务需求变更、原有系统改造等导致的问题除外）。

4. 除外责任

以下情况不属于本规范约定的质保服务范围，乙方可根据甲方需求提供有偿服务：

因甲方人员违规操作、误操作导致的设备损坏、软件故障或系统异常；

因自然灾害（如地震、洪水、雷击等）、意外事故（如火灾、停电等）、第三方破坏等不可抗力或外部因素导致的系统故障；

甲方擅自对设备进行拆卸、改装、更换零部件，或对软件进行破解、修改、未授权升级等操作导致的问题；

超出合同约定范围的新增功能需求、系统扩容、业务变更等产生的服务；

因甲方使用非正版软件、未经认证的硬件设备导致的兼容性问题或系统故障；

其他非乙方产品质量或服务缺陷导致的问题。

（三）质保服务要求

1. 服务响应与故障处理

（1）设备制造商在郑州境内设有正规维修点和维修机构及必需的零部件备件库；

（2）质保期内提供 7×24 小时技术支持服务，接到故障报修通知后，需在 2 小时内响应，明确故障处理方案：一般故障 48 小时内解决，重大故障 72 小时内解决；

（3）若故障检修后仍无法排除的，乙方应提供不低于故障规格型号档次的替代产品供甲方使用，直至原产品故障排除为止；若乙方未能在产品故障报修后三个月内排除故障的，需在三个工作日内更换不低于原产品型号、质量、配置、性能和售后服务的产品；

（4）质保期内出现软硬件质量问题需要更换设备时，乙方负责免费尽快更换，并赔偿因此给甲方造成的损失；维修或更换所发生的一切费用（含工时费、交通费、住宿费、通讯费、运输费等）均由乙方承担。

2. 软件升级与维护

（1）质保期内免费提供软件功能升级服务，及时响应甲方基于业务需求的合理功能优化建议（不涉及重大功能变更）；

（2）定期对软件系统进行巡检，及时发现并修复潜在问题，确保系统稳定运行；巡检完成后提交巡检报告，说明系统运行状态及处理的问题。

3. 技术支持与培训

（1）质保期内提供无偿的技术支持服务；

（2）乙方提供完善的技术培训服务，包括但不限于系统操作、日常维护、故障排查等内容，培训对象覆盖甲方相关管理人员及操作人员，确保相关人员能熟练使用系统；

(3)提供长期技术咨询服务，通过电话、邮件、远程协助等方式解答甲方在系统使用过程中的疑问。

4. 质保期满后服务要求

(1)质保期满后，乙方需提供长期、稳定的售后服务，包括设备维修、备件供应、软件维护等，收费标准应合理、透明，提前与甲方协商沟通；

(2)保证长期供应零备件，备件价格不高于市场同期合理价格。

（四）质保责任

1. 乙方未按本规范提供质保服务的，甲方有权要求其限期整改；

2. 乙方提供的产品为非原厂正货、次品、旧品、水货或侵犯知识产权的产品的，需在三个工作日内更换合格产品，并承担由此给甲方造成的全部损失。

附件5：网络与信息安全承诺书

网络与信息安全承诺书

甲方应按照《中华人民共和国网络安全法》等法律法规的要求，履行相关网络安全义务，承担网络安全责任。

第一条 甲方承诺不利用乙方提供的服务进行下列任何活动或发布、传播下列任何信息：

（1）从事危害国家安全、泄露国家秘密等犯罪活动；从事国家法律、法规、政策所禁止的活动或违背公共道德的活动；

（2）散布谣言，扰乱社会秩序，破坏社会稳定；散布垃圾邮件、病毒程序；黑客行为；侵权行为；博彩、赌博游戏等；

（3）危害国家安全、泄露国家机密、颠覆国家政权、破坏国家统一的信息；损害国家荣誉和利益的信息；煽动民族仇恨、民族歧视、破坏民族团结的信息；违反国家宗教政策的信息；宣扬邪教和封建迷信的信息；淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的信息；侮辱或者诽谤他人，侵害他人合法权益的信息；妨碍互联网运行安全的信息；其他有损于社会秩序、社会治安、公共道德的信息或内容；

（4）发布、传播其他违反国家法律、法规、政策内容的。

甲方同时承诺不为他人从事上述活动或发布、传播上述信息提供任何便利，如因甲方违反上述约定产生的一切责任和后果均由甲方承担。甲方认可乙方有权判断本协议项下甲方从事的活动或甲方发布的信息是否违法、违规或违反本协议有关规定，且乙方有权在提前通知甲方的情况下采取一切必要措施，包括但不限于暂停或终止提供本协议项下的服务、要求甲方进行整改等，但乙方上述权利不应被视为乙方有审核甲方行为或信息内容的义务或保证其合法合规的任何责任。

第二条 甲方不得有下列危害电信网络安全和信息安全的行为：

（1）对电信网络的功能或者存储、处理、传输的数据和应用程序进行违法删除或者修改。

（2）利用电信网络从事窃取或者破坏他人信息、损害他人合法权益的活动。

（3）故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施。

（4）危害电信网络安全和信息安全的其他行为。

若甲方存在上述任一情形的，乙方有权按相关规定暂停或停止提供服务、断开网络接入，保存有关记录，并向政府主管部门报告，由此引起的一切后果和责任由甲方负责。同时，乙方有权终止合同，并不承担任何责任。

第三条 甲方不得将接入设备转借或租赁给其它单位和个人使用，以防止非法信息的传播；否则，由其承担相关责任，乙方有权立即停止相关服务。

第四条 甲方应承担如下管理责任：

（1）向所属员工或使用者宣传国家及电信主管部门有关电信安全的法规规定。

（2）建立健全使用者档案，加强对使用者的管理、教育工作。

（3）有健全的网络安全保密管理办法。

第五条 甲方有责任对其自身系统的网络安全状况负责，并定期对其系统的安全状况进行检查，若发生网络攻击、信息泄露等网络安全事件，乙方不承担相关责任。

第六条 甲方侧数据由甲方负责，如出现信息泄露、信息篡改等安全事件，乙方不承担责任。

第七条 甲方承诺采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。不得从事以下行为：

（1）利用自己或他人的机器设备，未经他人允许，通过非法手段取得他人机器设备的控制权；

（2）非授权访问、窃取、篡改、滥用他人机器设备上的信息，对他人机器设备功能进行删除、修改或者增加；

（3）向其他机器设备发送大量信息包，干扰其他机器设备的正常运行甚至无法工作；或引起网络流量大幅度增加，造成网络拥塞，而损害他人利益的行为；

（4）资源被利用进行网络攻击的行为或由于机器设备被计算机病毒侵染而造成攻击等一切攻击行为。

（5）有意通过互联网络传播计算机病毒；

（6）因感染计算机病毒进而影响网络和其它客户正常使用的行为。

第八条 甲方业务如使用乙方提供的 IP 地址，甲方需承诺并确认：甲方所提交的所有备案信息真实有效，且备案信息不得出现乙方任何内容。当提供的备案信息发生变化时应及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，乙方有权依法采取停止提供服务、断开网络接入等关闭处理措施。如因甲方原因造成信息未及时通知，引发相关网络信息安全事件的，由甲方自行承担相关责任。

甲方签字盖章：

年　　月　　日