合同书

项目名称：梧州市公安局天网后端设备机房租赁托管服务采购项目

项目编号:WZZC2025-G3-990237-GXXK

日期：二 O 二五年十一月

梧州市公安局天网后端设备机房租赁托管服务采购项目

采购合同

采购计划号：WZZC2025-G3-02167001、WZZC2025-G3-02167002

合同编号：WZZC2025-G3-990237-GXXK

采购人（甲方）：梧州市公安局

供应商（乙方）：中国移动通信集团广西有限公司梧州分公司

项目名称：梧州市公安局天网后端设备机房租赁托管服务采购项目

项目编号：WZZC2025-G3-990237-GXXK

签订地点：广西梧州市　　签订时间：2025.11.13

本合同为中小企业预留合同：（是/否）。

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照磋商文件规定条款和乙方响应文件及其承诺，甲乙双方签订本合同。

第一条　合同标的

1、项目一览表

序号	项目名称	服务内容	数量	单位	单　价（元/月）	月总价（元/月）	合同期	合同期总价（元）
1	梧州市公安局天网后端设备机房租赁托管服务项目	1、包含70个机柜租用(包括电费及环境用电等)，其中市局在用45柜，备用9柜;交警在用11柜，备用5柜。便于后期机柜需求的扩容，单机柜空间≥44U(可完全利用)单机柜设计功耗≥4千瓦，满足TIER3保障级别。	70	个	1850	129500	24个月	3108000
2		2、提供1条网络带宽不低于3Gbps的全光纤数据专线(两端地址:托管机房至梧州市公安局负一层机房)。	1	条	5500	5500		132000
人民币合计金额（大写）：叁佰贰拾肆万元整（¥3240000）								

2、合同合计金额包括但不限于供应商提供本项目所需服务内容、所需场所、工具、安

装、调试、验收、培训、电费、服务人员等各种费用、售后服务、税金及其它不可预见等一切费用的总和，对于本文 件中未列明，而投标人认为必需的费用均包括在合同金额内。如招标文件对其另有规定的，从其规定。

第二条　质量保证

乙方所提供的服务及服务内容必须与投标文件承诺相一致，有国家强制性标准的，还必须符合国家强制性标准的规定，没有国家强制性标准但有其他强制性标准的，必须符合其他强制性标准的规定。

第三条　权利保证

1、乙方应保证所提供服务在使用时不会侵犯任何第三方的专利权、商标权、工业设计权等知识产权及其他合法权利，且所有权、处分权等没有受到任何限制。

2、没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方的保密义务持续有效，不因为本合同履行终止、解除或无效而解除。

第四条　交付和验收

1、交付使用时间：　自签订合同之日起 30 日内，完成本次租赁服务中所有涉及的机房租用、网络数据链路、机柜提供等部署工作（若因供应商提供的机房服务需要，或经采购人供应商双方协商一致，需将现有天网后端设备搬迁至本合同约定的新机房，供应商应负责将现有天网后端设备搬迁至新的机房运行，供应商负责在合同签订之日起 30 日内完成天网设备在新机房中的运行环境构建和调试，确保原有设备在拆除、搬迁及安装过程中安全无损。因供应商原因在搬迁过程中造成采购人设备损坏、数据丢失或业务中断超过约定时间的，供应商除负责修复、赔偿外，还应承担本合同第十条约定的违约责任。采购人除托管租赁服务费用外，不再因机房的整体搬迁、割接、布线、组网等工程支付额外的费用，搬迁工作须在 24 小时内完成并恢复所有天网设备正常运行），经采购单位验收确认后，完成交付进入服务期。如中标方无法按时交付使用，采购人有权选择终止合同向中标方追索超期时间段的天网后端设备租赁支出。交付地点：广西梧州市采购人指定地点　，租赁服务期：2 年　。

2、行业的国家标准、行业标准、地方标准或者其他标准、规范。

3、采购方将按相关行业标准对服务中所有涉及的机房租用、网络数据链路、机柜进行交付使用前阶段性验收，验收通过后才正式进入服务期。阶段性验收合格后由采购方和中标方签署验收单并加盖双方公章，双方各执一份。

4、阶段性验收过程中所产生的一切费用均由供应商承担。报价时应考虑相关费用。

5、在服务过程中，采购方每 3 个月对中标方考评一次。

第五条　售后服务及培训

1、乙方应按照国家有关法律法规和本合同所附的《售后服务承诺》及招标文件要求为甲方提供相应的售后服务。

2、乙方负责甲方有关人员的培训。培训时间、地点：甲方指定时间、地点 。

第六条　服务考评

本项目服务每满三个月为一个周期，每周期考评一次，具体内容如下：

一、天网后端设备托管的考评标准

事故类别	事故类别定义
一般事故	因机房环境（包括但不限于断电、环境温度过高、雷电、火灾、漏水、机房电线短路等）造成天网平台中断故障的，（因业主单位存在单电源设备导致断电除外）： 中断时间 60 分钟＜T＜90 分钟的事件发生次数≧1； 中断时间 T＜60 分钟的事件发生次数≧3； 满足以上 2 点情况的其中一点，视为一般事故。
重大事故	因机房环境（包括但不限于断电、环境温度过高、雷电、火灾、漏水、机房电线短路等）造成天网平台中断故障的，（因业主单位存在单电源设备导致断电除外）： 中断时间 90 分钟＜T＜8 小时的事件发生次数≧1；满足以上情况的视为重大事故。
严重事故	1、机房环境（包括但不限于断电、环境温度过高、雷电、火灾、漏水、机房电线短路等）造成天网平台中断故障的，（因业主单位存在单电源设备导致断电除外）： 中断时间 T＞8 小时的事件发生次数≧1； 2、因机房的运行环境造成天网平台设备大规模损坏，并对我局的天网平台造成严重损失的； 满足以上 2 点情况的其中 1 点，视为严重事故。发生本项第 2 点的，我局有权要求服务商赔偿损失。

（1）考评周期内，无事故发生，本周期应结算租赁机柜服务金额=初步结算金额*100%。

（2）考评周期内，发生一般事故的，本周期应结算租赁机柜服务金额=初步结算金额*90%。

（3）考评周期内，发生重大事故的，本周期应结算租赁机柜服务金额=初步结算金额*80%。

（4）考评周期内，发生严重事故的，本周期视为服务不合格，扣减本周期应结算租赁机柜 100%服务费。

二、租用网络线路的考评标准

1、天网后端设备托管网络数据链路服务（托管机房-梧州市公安局）的网络中断时间 8 小时＜T＜24 小时的事件发生次数≧1，或租用的网络中断时间 T＜8 小时的事件发生次数≧3 的，视为一般网络事故，扣减本次考评周期内 10%的网络费用。

2、网络中断时间 24 小时＜T＜48 小时的事件发生次数≧1，视为重大网络事故，扣减本周期内 40%的网络费用。

3、网络中断时间 T＞48 小时的事件发生次数≧1；视为严重网线络事故，本周期考评不合格，扣减本周期内 100%的网络费用。

第七条　付款方式

1、本项目无预付款。

2、在服务期内采购人每 3 个月对服务考评一次（考评标准详见第六条服务考评），每半年按考评结果向中标供应商结算一次费用，其中：托管租赁费用按实际使用的机柜数量结算；梧州市公安局天网后端设备托管网络数据链路服务费用按使用月份数量结算。中标供应商向采购单位开出对应金额有效的增值税发票，采购单位收到发票后向中标供应商付清本次结算费用（不计利息）。

备注：

如机柜投入使用数量未达到 70 个，托管租赁费用按实际使用的机柜数量结算，机柜的租费以机柜投入使用月份开始计费（例如在 2025 年 9 月内新增 2 个机柜投入使用，这 2 个机柜的租费就在 2025 年 9 月起开始计费）。

当机柜投入使用数量达到 70 个后，为保证甲乙双方的合法权益，双方根据项目实际情况核实并调整。任何对本合同的补充、修改或变更，均须以书面形式经双方签署，并依据《中华人民共和国政府采购法》等规定履行必要的审批、备案程序后生效。

第八条　履约保证金（如有）

履约保证金金额：无履约保证金　。

第九条　税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第十条　违约责任

1、除不可抗力原因外，乙方没有按照合同规定的时间提供服务的，甲方可要求乙方支付违约金。每推迟一天按合同金额的 3‰支付 违约金，该违约金累计不超过合同金额的 10%。超过十个工作日甲方 有权解除合同，乙方应向甲方支付合同总金额 30%的违约金并承担因 此给甲方造成的经济损失。

2、乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷 或诉讼，均由乙方负责交涉并承担全部责任。若甲方因此而遭受损失 或甲方声誉因此受到严重不良影响的，甲方

有权解除合同，乙方除返 还全部合同款并按合同总金额的 30%向甲方支付违约金外，还应赔偿 甲方因此而遭受的全部损失。

3、乙方的售后服务未按本合同提供或技术支持与服务或提供的 服务未达到服务要求，甲方提出书面整改意见后，乙方仍未在规定时 间内完成整改，每出现一次乙方需向甲方支付合同金额的 0.1%的违 约金。如乙方无正当理由拒绝的，甲方有权聘请第三方进行维护，因 此产生的费用以及经济损失均由乙方承担。

4、如乙方违反合同要求的保密约定，每违反一次，视情节轻重， 扣除合同金额的 0.2%至 1% ，直至扣完合同金额为止，如合同款项 已支付，则甲方有权向乙方追回。若还给甲方造成其他损失的，还需 向甲方承担赔偿责任。

5、经济损失是指一方因此而遭受的全部经济损失（包括但不限 于直接损失、间接损失及实现债权的费用，如诉讼费、律师费、差旅 费、调查费、财产保全责任险保险费等）。

6、甲方有权从未付价款中先行扣除乙方应支付的违约金、赔偿 金，不足另补。

第十一条 不可抗力事件处理

1、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十二条 合同争议解决

1、因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权的人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十三条 通知和送达

1、各方确认，本合同载明的各方地址为各方真实有效通讯地址， 一方向对方发出的任何通知、信函和文件，以挂号信函或快递信函方 式向对方地址邮寄有关通知、信函和文件的，自发出之日起第三日视 为送达对方，挂号信函或快递信函的邮寄凭证即视为成功送达的有效 凭证。一方地址变更的，应在变更后 10 日内书面通知对方，否则本 合同载明的地址仍为真实有效通讯地址。若为专人提交的，自对方法 定代表人、授权代表、委托代理人签收时或单位盖章时视为送达对方。 因提供或者确认的通讯地址不准确、通讯地址变更后未及时依程序告 知对方或受送达方拒绝签收等原因，导致文书未能被实际接收的，邮 寄送

达的，以文书退回之日视为送达之日。

2、本合同载明的各方电子邮箱、微信号是各方真实有效的通讯 联系方式，一方向对方发出的任何通知、信函和文件，若以邮件方式发送的，自邮件发送成功视为送达对方，若以微信方式发送的，自微 信发送成功视为送达对方。一方电子邮箱或微信变更的，应在变更后 10 日内书面通知对方，否则本合同载明的电子邮箱或微信仍为真实有效的通讯联系方式。

3、上述送达地址和联系方式适用范围包括双方非诉时各类通知、合同等文件以及就合同发生纠纷时相关文件和法律文书的送达，同时包括在争议进入仲裁、民事诉讼程序后的一审、二审、再审和执行程序。

第十四条　合同生效及其它

1、合同经双方法定代表人或者授权代表签字并加盖单位公章后生效（委托代理人签字的需后附法定代表人授权委托书，格式自拟）。

2、合同执行中涉及采购资金和采购内容修改或者补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

第十五条　合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或者终止。

2、乙方不得擅自转让其应履行的合同义务。

第十六条　签订本合同依据

1、中标通知书；

2、投标文件中的相关文件。

3、上述合同文件互相补充和解释。如果合同文件之间存在矛盾 或者不一致之处，以上述文件的排列顺序在先者为准。

第十七条　本合同一式五份，具有同等法律效力，采购代理机构各一份，甲乙双方各贰份（可根据需要另增加）。

本合同甲乙双方签字盖章后生效，自签订之日起七个工作日内，甲方应当将合同副本报同级财政部门备案。

本合同自签订之日起 2 个工作日内，甲方应当将采购合同在广西壮族自治区财政厅指定的媒体上公告。

甲方：（章）梧州市公安局 2025.11.13 年 月 日	乙方：（章）中国移动通信集团广西有限公司梧州分公司 2025 年 11 月 13 日
单位地址：梧州市长洲区大旺路 66 号	单位地址：梧州市长洲区新兴三路 13 号
法定代表人：	法定代表人：
委托代理人：	委托代理人：
电话：	电话：
开户银行：中国工商银行梧州市红岭支行	开户银行：中国工商银行股份有限公司南宁市琅东支行
账号：2104320829100008829	账号：9558852102001168849
邮政编码：543000	邮政编码：543000
纳税人识别号：114504000076662780	纳税人识别号：91450405715116322F

合同附件

附件一：中国移动互联网数据中心管理规范
附件二：中国移动 IDC 客户信息安全责任承诺书
附件三：IDC 服务等级承诺（SLA）
附件四：数据安全风险防范告知书
附件五：互联网数据中心网络和数据安全能力需求
附件六：数据安全协议（如涉及数据处理）
附件七：商务需求响应表、服务需求响应表

附件一：中国移动互联网数据中心管理规范

中国移动互联网数据中心管理规范

凡访问和使用中国移动互联网数据中心（下称数据中心）设施和其中系统的人士（数据中心员工除外），必须遵守以下的各项规定，确保数据中心系统的安全。

一、访问数据中心

1. 必须出示有效身份证明和文件，证明进入数据中心已经过授权。
2. 参观人员必须事先报经数据中心人员同意后，在数据中心人员带领下，方可进入。
3. 进入数据中心必须佩戴数据中心发出的访客标识。
4. 只能在授权活动范围内活动，不得随意在数据中心活动或擅自进入机房。
5. 除特别需要外(如系统安装，更换服务器，更换硬件)，维护人员不得进入机房进行调试。
6. 维护人员进入机房在维护工作完成后，应立即离开机房，不得无故停留。
7. 重启进程等工作，可以选择远程操作，如有特殊需求，可在数据中心指定调试工位进行调试，调试过程中禁止做与工作无关的操作。
8. 配合数据中心相关维护管理人员，填写相应登记记录，并告知数据中心维护管理员进入机房的维护内容，得到允许后，方可进入机房。
9. IDC 客户放入机房的服务器必须是品牌设备（产品具有 SN 号，并且可以在官方网站上查询到）。

二、在数据中心的行为

1. 不得：
   - 使用、误用或滥用任何数据中心系统或其它数据中心使用者的设备或系统；
   - 未经授权使用或干扰其他数据中心使用者的财产、设备、系统；
   - 干扰、骚扰他人，包括数据中心人员或数据中心在场其他人员；

- 从事违反法律法规的任何活动或协助其他人员进行违反法律法规的任何活动；
- 在系统调试过程中浏览网页、聊天、查看新闻等做任何与工作无关的事情；
- 未经事先允许或无数据中心人员陪同而进入数据中心核心区；
- 随意安装、摆放设备。

2. 设备摆放须遵守数据中心机房管理要求。为保障设备正常运行，机柜内需留有散热空间，机柜设备安装应符合机柜设备安装规范要求，不符合机柜设备安装规范要求的，须按照中国移动要求配合整改。
3. 保持数据中心清洁。

   不得：

   - 将未与数据中心书面确定的任何设备放入数据中心；
   - 在数据中心内存放任何纸制品或任何性质的其它易燃材料（设备手册除外）；
   - 随便开启门户或者容许其他人士进入数据中心。
   - 使用任何拍照，摄像或录像设备在数据中心进行摄像/录像。
   - 违反其他相关管理规定或不利于数据中心正常工作运行的行为；
4. 不得将以下或类似物品（违禁材料）带入数据中心：
   - 食品和饮料，烟制品，爆炸物、武器、刀具等危险物品；
   - 易燃、易爆、污染等危险材料；
   - 酒精、非法药物和其它麻醉剂；食品和饮料，烟制品，
   - 干扰或可能干扰计算机和通信设备的电磁设备；
   - 用于访问技术系统的任何直拨或回拨调制解调器；
   - 任何恶意软件或代码；
   - 放射性材料；
   - 违反其他相关管理规定或不利于数据中心正常工作运行的物品；

数据中心有权监控任何人在数据中心内的全部活动，对违反此规范文件或任何法规者采取适当的行动，包括但不限于要求有关人员马上离开、取消其一切授权、或把情况报告司法机关。

在法律允许范围内，本管理规范的解释权属于乙方，乙方有权不时对本管理规范进行调整或变更，但变更后的规范需甲方书面确认同意后方能适用于客户。

附件二：中国移动 IDC 客户信息安全责任承诺书

为切实加强 IDC 接入客户的安全使用和规范管理，促进互联网信息服务活动健康有序发展，维护国家安全和社会稳定，保障社会公众利益和公民合法权益，保障其它客户的合法权益，中国移动通信集团公司及中国移动通信有限公司（下文统称中国移动）根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》和其他相关法律、行政法规的规定，结合中国移动现有 IDC 接入业务和网络现状制定本安全责任承诺书。

我单位对于所申请的中国移动通信有限公司及其下属子公司（以下简称“中国移动”）的互联网接入服务（包括但不限于 IDC 业务、互联网接入业务等将内容引入到中国移动网内的业务），为确保向客户提供健康的信息服务，明确企业主体责任和法律责任，向中国移动郑重承诺如下：

一、遵守国家有关法律法规，提供的信息符合国家法律、法规与工业和信息化部等政府部门的各项管理规定以及中国移动《IDC 信息安全管理规范》的相关规定，并严格执行上述信息安全管理规定。

二、不得利用中国移动互联网（CMNET）从事危害国家安全、泄露国家机密等违法犯罪活动，不得利用中国移动互联网（CMNET）制作、查阅、复制和传播违反宪法和法律、妨碍社会治安、破坏国家统一、破坏民族团结、色情、暴力等的信息，不得利用中国移动互联网（CMNET）发布任何含有下列内容之一的信息：

1、危害国家安全、泄露国家秘密，侵犯国家的、社会的、集体的荣誉、利益和公民的合法权益，从事违法犯罪活动；

2、煽动抗拒、破坏宪法和法律、行政法规实施的；

3、煽动颠覆国家政权，推翻社会主义制度的；

4、煽动分裂国家、破坏国家统一的；

5、煽动民族仇恨、民族歧视，破坏民族团结的；

6、捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

7、破坏国家宗教政策，宣扬邪教、封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

8、公然侮辱他人或者捏造事实诽谤他人的；

9、损害国家机关信誉的；

10、其他违反宪法和法律、行政法规的；

11、侵犯他人知识产权，传播虚假信息的；

12、违背社会主义精神文明建设要求、违背中华民族优良文化传统与习惯、以及其它违背社会公德的各类低俗信息。

三、不得利用中国移动互联网（CMNET）从事以下破坏计算机系统及互联网安全的行为：

1、网络攻击行为

1）利用自己或他人的机器机器设备，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。

2、淫秽色情信息危害行为

1)在网站或业务平台等相关系统发布、传播淫秽色情和低俗信息的行为；

2）网站或业务平台引入、分发其他的网站、应用等内容，由于管理、手段缺失，而导致引入、分发内容包含色情、低俗等不良信息的行为。

3、计算机病毒危害行为

1）有意通过互联网络传播计算机病毒；

2）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。

4、发送或协助发送垃圾邮件行为

1）故意向未主动请求的客户发送或中转电子邮件广告刊物或其他资料；

2）故意发送没有明确的退信方法、发信人、回信地址等的邮件；

3)邮件服务器存在安全漏洞或开放 OPENRELAY 功能导致被利用转发垃圾邮件；

4）冒名发送恶意邮件（违反国家法律法规的）；

5）其它任何协助垃圾邮件发送行为、可能会导致影响网络正常运营及其它客户正常使用的邮件等。

5、手机恶意软件危害行为

1)服务器作为手机应用软件下载源所提供的下载列表中含有违规恶意软件，或者直接作为手机恶意软件的下载源，通过互联网传播手机恶意软件；

2）作为手机恶意软件控制服务器，对中毒用户手机进行远程控制，进行下发远程指令、收集用户隐私、不知情定制业务造成扣费等恶意行为。

四、发现上述违法犯罪活动和有害信息，应立即采取措施制止并及时向有关主管部门报告。对于其它破坏中国移动网络信息安全或违反国家相关法律法规规定的行为，本责任书同样适用。

五、我单位承诺对在中国移动接入的业务网站、即时通信工具、网盘、视频等进行全面检查、逐一过滤，彻底清理涉暴恐音视频等存量有害信息，关闭传播恐怖宣传视频的注册账户，并建立清理暴恐音视频工作台账。

六、我单位采取必要手段加强网站/平台内容监测、审核、拦截，一经发现涉暴恐音视频等有害信息，立即清理，并及时上报国家相关部门。

七、我单位在联网测试、试运行期间、业务正式开通以及合作业务推广过程中，遵守中国移动相关管理规定，保证所提供业务内容的安全性与稳定性，不对中国移动通信网络、相关业务平台造成危害。

八、我单位保证建立有效的信息安全管理制度和技术保障措施，并接受相关主管部门的管理、监督和检查，为相关主管部门提供技术支持。

九、中国移动将通过技术手段、受理投诉及其它方式实时监控中国移动 IDC 网络及内容信息的安全状况。对于违反国家相关法律法规的客户、不采取相应措施保证自身网络及内容信息安全的客户、恶意威胁中国移动 IDC 网络安全的客户以及妨碍其他 IDC 客户正常使用的客户等，中国移动将依据国家相应法规、条例以及本责任书内容采取相应处理措施以保证网络的安全。情节严重者，将报送当地司法机关进行处理。

十、中国移动作为电信运营商，有按要求配合国家有关部门处理互联网网络与信息安全工作的义务，包括但不限于提供客户基础资料、采取技术措施处理

等。

十一、中国移动在接到投诉或发现危害互联网安全的行为后，将立即针对不同情况予以处理，直至确认客户已完成有效整改：

1、危害信息安全的行为：立即对非法信息源、传播途径以及互连端口等进行封堵，并进行封存取证。

2、网络攻击行为：立即针对其攻击途径、端口进行封堵，并进行封存取证。对于相关人员视情节轻重采取相应处理措施，直至移交国家信息安全机构及当地司法机关依法处理。

3、淫秽色情信息危害行为：立即删除淫秽色情和低俗信息，并查找原因分析不足，对发布的信息建立完善的审核、管控机制，进行事前审核、事中监控、事后处置，防止出现淫秽色情和低俗信息；对非法信息源、内容引入路径等进行封堵，禁止引入、发布包含淫秽色情和低俗内容的域名链接。对网络安全影响严重，可能或已经造成中国移动 IDC 网络及其他客户损失时，中国移动将立即中断客户网络连接，同时以多种方式通知客户。对于相关人员视情节轻重采取相应处理措施，直至移交国家信息安全机构及当地司法机关依法处理。

4、计算机病毒危害行为：在接到投诉或警示发现此行为后，接入客户应首先断开与中国移动网络的连接并及时清除计算机病毒。若接入客户在接到警示后 30 分钟内没有采取措施改正，或被发现的计算机病毒已被证实或有理由相信其危害性对网络安全影响严重，可能或已经造成中国移动 IDC 网络及其他客户损失时，中国移动将立即中断客户网络连接，同时以多种方式通知客户。

5、发送或协助发送垃圾邮件行为：在接到投诉或警示发现此行为后，将立即对入驻客户予以警告，并列入监控名单；对于情节严重者，将立即针对参与发送或协助发送垃圾邮件的客户暂时关闭网络服务及对互连端口进行封堵。

十二、对屡整屡犯、明知故犯的，中国移动有权单方面中止双方 IDC 接入合作协议；情节严重的将移交国家信息安全机构、当地司法机构等相关部门并依法配合处理。对于对中国移动 IDC 造成重大经济损失和名誉影响的，中国移动有权追究经济赔偿和法律责任。

十三、所有签署本责任承诺书的客户必须认同中国移动对危害互联网安全行为的定义，并承诺承担以下责任和义务：

1、自觉遵守国家有关互联网管理的法律、法规，建立有效的网络安全与信息安全管理制度和技术保障手段及措施。

2、按照中国移动 IDC 网络安全行为类型，对自身网络行为和其下挂客户的网络使用行为进行管理和约束。

3、接受中国移动相关部门的管理、监督和检查，接受中国移动 IDC 网络与信息安全工作的处理方法，有责任和义务积极配合中国移动查找、清除非法网络行为，直至处理完毕。

4、对自身网络行为和其下挂客户的网络使用行为负全责，承担相应的经济责任和法律责任。

5、联系方式或网络安全责任人发生变更时，应及时通知中国移动相关联系人员，否则导致的一切后果由客户自身承担。

十四、“依据《非经营性互联网备案管理办法》第二十三条规定，如备案信息不真实，将关闭网站并注销备案。入驻客户承诺并确认：提交的所有备案信息真实有效，当备案信息发生变化时请及时与中国移动 IDC 域名备案部门联系并提交更新信息，如因未及时更新而导致备案信息不准确，我公司有权依法对接入网站进行关闭处理。

十五、如有其它影响网络安全和信息安全的突发事件，中国移动有权采取紧急措施，以保证网络安全。

十六、如果出现未知原因的攻击导致系统设备性能、网络流量或网页内容异常，产生严重后果时，中国移动有权在不提前通知我单位的情况下采取一切必要措施。

十七、若违反上述规定，中国移动有权采取措施，关闭相关信息源接入通道；同时，追究责任单位的法律责任，并且终止与责任单位的合作。

本安全责任承诺书作为对应 IDC 合同的附件，与该合同具有相同的法律效力。

我单位愿承担上述各项信息安全管理责任，积极配合中国移动公司做好 IDC 网络及信息安全管理工作。若违反上述规定，中国移动有权采取措施，对责任

单位进行经济惩罚以及关闭相关信息源接入通道；同时，追究责任单位的法律责任，并且终止与责任单位的相关业务。此承诺书经我单位签署盖章后生效，并由中国移动负责保管。

特此承诺。

单位全称： 梧州市公安局

法定代表人或授权委托人姓名：

单位地址：梧州市长洲区大旺路 66 号

联系人姓名：

联系人电话：

单位公章：梧州市公安局

[日期]：

2025.11.1

附件三：IDC 服务等级承诺（SLA）

IDC 服务等级承诺（SLA）

为规范乙方向甲方提供的数据中心相关服务品质，乙方向甲方承诺提供如下 IDC 服务等级标准(SLA)：

一、基础设施保障

1. 乙方必须保证电力的持续供应：即保证向甲方提供的市电或 UPS 具有电力。乙方保证向甲方信息系统的电力的年度持续供应达 99.9%(百分之九十九点九)的可用性，即甲方托管的信息系统每年电力中断时间累积不超过 525.6 分钟。

   “电力中断”是指：乙方向甲方提供的市电及 UPS 电源同时不具有电力。

2. 乙方根据甲方要求，为甲方计算每年“电力中断”时间，“电力中断时间”指乙方造成的甲方信息系统电力中断的时间（分钟数），其不包括由以下原因引起的电力中断：

   1) 任何的甲方电路或设备；

   2) 甲方的应用、安装或维护活动；

   3) 甲方的疏忽或乙方按甲方授权进行的操作；

   4) 不可抗力原因所引起的；

   5) 政府或者电力公司要求的停电、限电；

   6) 计划停电；

   7) 其他本协议约定的免责情况。

3. 每年电力中断时间的确定须经甲方、乙方双方确认，如有争议，由双方协商解决。

二、网络联通性保障

1. “网络联通性”指甲方托管于乙方机房的网络设备与乙方网络、其他运营商网络、互联网是否联通。“网络联通”指乙方分配给甲方的网络端口可以与乙方网络、其他运营商网络、互联网相联通；“网络不联通”指乙方分配给甲方的网络端口与乙方网络、其他运营商网络、互联网不联通。

2. 乙方保证年度网络系统 99.9%(百分之九十九点九)的联通性。

3. 网络不联通时间的确定须经甲方、乙方双方确认，如有争议，由双方协商解决。

三、初装保障

1. 乙方承诺提供的初装服务内容应满足甲方的要求,具体包括以下内容：

1） 机房地面、墙面装修施工；

2） 电力供应的安装；

3） 网络连接的安装；

4） 空调设备的安装；

5） 隔断的安装；

6） 机柜的安装。

四、技术支持保障

1. 乙方将向甲方提供必要的技术支持，具体事项包括以下内容：

1） 7x24x365 基础设施运行维护；

2） 7x24x365 机房环境监控；

3） 7x24x365 安保服务；

4） 7x24x365 紧急情况通知；

5） 技术问题咨询。

2. 乙方须向甲方提供至少 1 名项目经理准确的联络信息，负责协调甲方与乙方机房运维相关的一切事宜。

3. UPS、供配电、空调等系统发生故障，乙方技术工程师应在发生故障 15 分钟内响应，在发生故障 1 小时内及时向甲方反馈故障情况，并在发生故障 1 天之内解决故障；乙方技术工程师应在故障解决后 3 天之内向甲方提交故障报告。

五、服务保障

1. 客户服务保障

乙方将指定 1 名客户经理对甲方进行全程跟踪服务，具体服务包括以下内容：

1） 服务项目和业务项目的咨询；

2） 初装工作受理及工作情况汇报；

3） 服务内容变更处理；

4） 投诉受理及处理情况汇报；

5） 缴费咨询及办理；

6） 了解、反馈并妥善处理甲方的需求。

乙方为甲方指定的客户经理，应保证 7x24x365 及时响应。

2. 机房开放保障

1） 乙方保证 IDC 机房全天 24 小时（除不可抗力外）向甲方开放，在甲方遵守机房管理规定及合同约定的前提下，可随时要求进入机房对其设备进行合理的操作。

2） 为保证 IDC 机房的安全，甲方需向乙方机房的管理人员提供甲方工作人员有效证件（机房出入许可证、身份证等），乙方人员验证无误后，甲方工作人员方可入内。甲方工作人员出入 IDC 机房应遵守 IDC 机房的有关规定。

3. 投诉保障

甲方可以书面或电话形式就以下问题对乙方某个员工投诉：

1） 网络品质；

2） 技术支持质量；

3） 客户服务质量。

4. 乙方设立投诉专线受理甲方投诉。

5. 乙方在受理甲方投诉后一个工作日内向甲方提供第一份书面形式的投诉处理报告。

六、配套服务保障

1. 乙方应提供保洁服务，对园区环境、公共设施和机房进行定期清洁。

2. 乙方应设置泊车场所，提供免费的泊车服务。

附件四：数据安全风险防范告知书

数据安全风险防范告知书

为落实《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》《中华人民共和国网络数据安全管理条例》等相关法律法规，维护数据安全生态，保障数据主体合法权益，防范数据泄露、滥用、篡改等安全风险，特向贵单位发出《数据安全风险防范告知书》。

一、数据安全风险提示

贵单位在业务系统运行过程中，可能面临以下数据安全风险（包括但不限于）：

1. **数据泄露风险：**数据传输、存储或共享过程中可能因网络攻击、系统漏洞、人为误操作等导致数据泄露。

2. **数据滥用风险：**第三方服务商或内部人员可能超出约定用途使用数据（如非法营销、转售等），引发法律纠纷。

3. **数据篡改风险：**数据可能因恶意攻击或系统故障被篡改，影响业务决策与数据可信度。

4. **跨境传输风险：**数据跨境传输需通过国家网信部门安全评估，擅自传输可能导致行政处罚及用户索赔。

5. **供应链风险：**第三方供应商（如云服务商、开发团队）安全管理能力不足，可能间接导致数据泄露或违规使用。

二、数据安全建议

为降低上述风险，建议贵单位根据法律法规及业务需求，采取以

下管理和技术措施：

1. **落实数据分类分级管理：**对业务涉及的个人信息、重要数据等进行分类标识，优先加密或脱敏处理敏感数据。

2. **强化技术防护：**采用数据加密（如 TLS/SSL）、访问控制、日志审计等技术手段，根据数据级别实施差异化安全管理，防范未授权访问。

3. **完善权限管理：**遵循最小必要原则分配数据访问权限，及时回收离职人员账号权限。

4. **规范第三方合作：**与第三方服务商签订数据保护协议，明确数据使用范围及安全责任。

本单位已完整阅读并充分理解《数据安全风险防范告知书》的全部内容，承诺严格遵守国家法律法规及双方协议约定，切实履行数据安全保护义务。

单位（盖章）：梧州市公安局

法定代表人或授权经办人（签字/盖章）：

日期：2025年11月13日

附件五：互联网数据中心网络和数据安全能力需求

注：以下涉及客户数据的能力可能需要委托中国移动广西公司对客户服务器内的数据进行处理

种类	序号	能力名称	功能概述	安全能力分类	是否接触客户数据	是否需要在客户服务器部署软件	是否属于增值业务	是否愿意对接广西移动安全能力平台
等保合规	1	下一代防火墙	全面应对应用层威胁的高性能防火墙，可提供互联网边界和内网 VPC 边界的流量管理与安全防护，具备 IP 五元组安全访问控制、入侵防御、病毒防御、僵尸网络防御等能力。	流量型	否	否	是	□是 ☑否
	2	入侵防御	深度解析并准确发现各类非法入侵攻击行为并阻断。具备漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、暴力破解，网络层分析到应用层分析能力。		否	否	是	□是 ☑否
	3	Web 应用隔离	WEB 应用隔离利用远程浏览器隔离技术（RBI）对被保护网站进行转码，并通过私有协议向访问用户呈现基于原网站的镜像网页，可较好地隐藏暴露面漏洞，从技术上隔离漏洞和攻击。		否	否	是	□是 ☑否
	4	数据库审计	针对数据库操作行为进行细粒度审计的合规性管理系统。它通过各类数据库访问行为进行解析、分析、记录、汇报，用来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，同时加强内外部行为监管、促进核心资产的正常运营。	客户端型	是	是	是	□是 ☑否
	5	终端安全 EDR	终端安全 EDR 由轻量级的端点安全软件(Agent)和管理平台软件两个关键部分组成，支持终端资产管理和安全合规检查，可支持防病毒、微隔离和安全事件的一键隔离处理。		是	是	是	□是 ☑否
	6	网页防篡改	网页防篡改可实时监控网站目录或文件，并可在网站被恶意篡改时通过备份数据恢复被篡改的文件或目录，防止网站被植入非法信息，保障网站正常运行。		是	是	是	□是 ☑否
	7	安全升级	通过自动检测客户端漏洞并推送补丁更新，支持多系统版本适配，结合数字签名验证与灰度发布机制，保障软件更新安全可靠，减少漏洞被利用风险，满足合规要求。		否	是	是	□是 ☑否
	8	数据备份与恢复	根据不同类型数据的重要程度配置适当的备份方式，当原数据发生丢失或损坏时可通过技术手段将备份的数据还原到应用主机或系统，实现应急恢复，保障数据的可用性及业务连续性。		是	是	是	□是 ☑否

	9	日志审计	通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。	路由可达型	是	否	是	□是 ☑否
	10	堡垒机	安全运维管理系统（堡垒机）集单点登录、账号管理、身份认证、资源授权、访问控制和操作审计等为一体，支持多种字符终端协议、图形终端协议、文件传输协议和远程应用协议的运维操作、安全监控和审计分析，安全合规的运维安全审计产品。		是	否	是	□是 ☑否
	11	漏扫	漏扫提供 web 应用漏扫、系统漏扫和基线核查能力，通过资产自动化识别、漏洞及弱口令检测、紧急漏洞快速响应等手段，为用户提供持续的安全风险评估服务。		否	否	是	□是 ☑否
增强安全业务	12	资产测绘	资产测绘系统是集资产普查、风险探测、风险管理于一体的网络资产探测平台。系统支持对网络资产进行存活状态快速探测，并结合漏洞发现检测技术和数据情报分析技术，实现全网各类资产精准发现、精准识别、精准威胁检测的能力。		否	否	是	□是 ☑否
	13	网站安全监测	网站安全监测是一款针对大规模网站/网站群的安全状态进行全方位实时监控的产品，产品监测内容包括敏感词、网页木马、暗链、网页变更、网站可用性、域名劫持检测等。		否	否	是	□是 ☑否
数据安全	14	数据脱敏	数据脱敏系统可对多种类型数据源的敏感数据进行自动识别，按脱敏规则进行敏感数据匿名化处理，保证脱敏后的数据与其原始数据格式和属性保持一致，确保应用程序可使用脱敏后的数据正常进行开发与测试。	数据安全型	是	否	是	□是 ☑否
	15	数据分类分级	数据分类分级系统根据行业的业务数据特征和分类分级规范，提供行业模板，通过敏感数据识别技术全面、快速、准确发现和定位敏感数据，构建持续更新的企业敏感数据分类分级目录。		是	否	是	□是 ☑否
	16	数字水印	数字水印对外发数据进行添加数据标记、自动生成水印、数据源追溯等功能，避免了内部人员外发数据泄露无法对事件追溯，提高了数据传递的安全性和可追溯能力。		是	否	是	□是 ☑否
	17	数据安全网关	数据安全网关系统主要针对运维、研发测试、数据分析等内部人员实施数据库细粒度访问控制的主动防御型产品，主要包括数据内容的访		是	否	是	□是 ☑否

			问控制、访问审计、动态脱敏等安全防控技术。					
商用密码能力	18	签名验签	基于国密非对称算法的签名验签服务，支持多种签名格式，支持多种数据格式签名。能够对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并可验证签名数据和数字证书的真实性和有效性；满足用户在网络行为中的用户身份真实性鉴别、操作不可否认性等需求。	密码安全型	否	否	是	□是 ☑否
	19	时间戳	对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。		否	否	是	□是 ☑否
	20	协同签名	面向移动客户端替代传统 USB Key，提供数字签名功能，适用于 OA 协同、电子政务、移动办公、金融支付、健康医疗、移动端身份认证等多种场景。		否	否	是	□是 ☑否
	21	数据加解密	通过硬件密码机为业务系统提供高性能的密码运算能力和密钥管理能力。		是	否	是	□是 ☑否
	22	安全传输	在网银系统、支付平台、个人账户登录系统等需要处理敏感用户数据的场景下，使用国密 SSL/TLS 传输协议建立客户端和服务端之间的 HTTPS 安全传输通道，保护用户在不同网络环境下的数据传输安全。		是	否	是	□是 ☑否

附件六：数据安全协议（如涉及数据处理）

数据安全协议

双方恪守良好的职业道德，为确保合作过程中涉及的数据的安全保密，以及促进数据合法、有效利用，防止发生数据泄露事件，防范违法违规使用行为，自觉遵守《中国人民共和国网络安全法》、《中国人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等国家有关网络安全的方针政策、法律法规、行政规定。经双方协商一致，签订数据安全协议严格约束双方具体的数据合作范围和内容以及双方的权利与义务，达成如下协议（“本协议”）。

第一条 定义

1.1 数据：是指任何以电子或其他方式对信息的记录。数据包含个人信息和不包含个人信息的其他数据，如与网络及业务相技术规范、配置数据与拓扑、项目管理信息、源代码、企业信息等。

1.2 数据处理：是指数据的收集、存储、使用、加工、传输、提供、公开、销毁等环节。

1.3 技术支撑服务：是指为数据处理或使用提供必要的基础资源支撑、平台支撑或研发建模技术支撑等，不存在数据共享和对数据的处理行为。

1.4 数据产品：是指与数据相关的产品，包括提供技术支撑服务的产品、对数据进行加工处理形成的产品或者同时提供数据结合技术支撑服务的产品。

1.5 数据提供方：是指将其持有的数据全部或者部分对外提供的主体。

1.6 数据接收（使用）方：是指接收数据提供方提供的数据，根据自己的目的自行进行处理、接受数据提供方的委托进行处理，或者与数据提供方共同决定数据处理目的的主体。

1.7 敏感个人信息：是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、

特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

第二条 数据提供方的数据安全义务

2.1 数据提供方应保证提供给数据接收（使用）方的数据来源合法，并采取措施增加数据的准确性。

2.2 涉及提供个人信息的，数据提供方开展业务及服务时应保障个人信息主体的知情权和选择权，应根据法律法规要求的内容及形式，告知相关个人信息主体关于数据提供方拟向其收集和使用的个人信息范围、处理方式、处理目的等内容并取得同意或其他处理合法性基础。

2.3 数据提供方须保证数据主体授权的真实性，并妥善保存数据主体授权记录，以供发生争议时查验追溯。数据授权记录包括但不限于协议文本、信件、传真、电子邮件、电子数据交换等形式。具体如下：

（1）涉及提供个人信息的，数据提供方须保证相关个人授权的真实性，并妥善保存个人授权记录，以供发生争议时查验追溯。数据授权记录包括但不限于协议文本、信件、传真、电子邮件、电子数据交换等形式。

（2）涉及提供企业数据的，数据提供方应确保该数据的提供不违反与相关企业的保密协议等有关约定。

（3）对于因数据提供方未取得数据主体授权或授权不真实等引发的纠纷或诉讼，数据提供方承担全部责任。

2.4 当数据提供方委托数据接收（使用）方处理数据时，应尽职履行其监督义务，在职权允许范围内，采取包括但不限于审计、定期检查、听取报告等方式监督数据接收（使用）方的数据处理行为。双方应明确约定委托处理的目的、期限、处理方式、数据的种类、保护措施以及权利和义务等。在得知或者发现数据接收（使用）方未按照委托要求处理数据，或未能有效履行数据安全保护责任的，数据提供方有权要求数据接收（使用）方停止相关行为，且采取或要求数据接收（使用）方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制

或消除数据面临的安全风险。必要时，数据提供方有权终止委托关系，并要求数据接收（使用）方及时删除从数据提供方获得的数据。

2.5 当数据提供方提供的数据为重要数据或者核心数据时，应当在提供数据时及时向数据接收（使用）方告知，双方应当依据法律法规的要求对前述数据采取合法的处理行为及必要的安全保密技术措施。法律法规规定对于重要数据或者核心数据处理，需要评估安全风险，经行业监管部门审查后报监管部门提供的，由数据提供方评估后按照法律法规要求申报。

2.6 数据提供方在数据提供前，应对数据接收（使用）方开展资质审核与背景调查、安全保护能力评估、数据合作范围和权限最小化审核等工作；在开展数据业务合作时，数据提供方应与数据接收（使用）方签署具体业务合作协议，明确双方数据安全保护责任和义务。

2.7 数据提供方在数据提供时，应当根据法律规定，采取去标识化、加密等措施对个人信息进行脱敏处理，并采取必要的技术防护措施，防范个人信息转移过程中被除数据提供方和数据接收（使用）方之外的其他个人、组织截获和利用。对于无法脱敏的重要数据，通过技术验证数据处理者是否采取加密措施、选用安全可靠的传输协议、数据提供环境安全可控等必要的安全保障措施。

2.8 数据提供后，数据提供方应做好数据提供后的数据安全监督与检查工作。数据提供方有权要求数据接收（使用）方，对从数据提供方接收数据的合规处理情况以及安全技术管控措施进行说明。

2.9 数据提供方提供数据信息的行为不构成向数据接收（使用）方授予任何与数据信息相关的专利权、专利申请权、商标权、著作权、商业秘密或其它的知识产权、所有权或其他任何权利。

2.10 当数据提供方提供的数据为敏感个人信息时，应当在提供数据时取得个人的单独同意或其他处理合法性基础；法律、行政法规规定应当取得书面同意的，从其规定。当数据提供方处理的敏感个人信息中有不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意，并制定专门的个人信息处理规则。数据提供方还应当向个人告知处理敏感个人信息的必要性以及对

个人权益的影响。数据提供方应自行在提供前进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第三条 数据接收（使用）方的数据安全义务

3.1 数据接收（使用）方应按照法律法规的要求、合作文件的约定期限或在数据提供方明确要求时删除数据。双方一致确认，在不影响数据接收（使用）方正常业务开展的前提下，数据提供方有权且将采取所有可能、必要的手段对数据进行脱敏、模糊化、溯源水印标记等处理，数据接收（使用）方将被禁止对该等数据采取任何反向工程、反向编译或反向分解行为。

3.2 数据接收（使用）方同意只在与数据提供方约定的相对应的目的和范围内使用数据提供方数据。如涉及变更原先的处理目的、处理方式的，应当重新取得数据主体同意。

3.3 数据接收（使用）方不得违反有关法律法规以及数据提供方的各项网络信息安全和数据安全管理相关制度或规范以及本合同约定，以任何方式将数据的部分或全部披露、公布、散布、分发或转售给除了因工作需要必须使用该数据的人员之外的任何第三方，且提供范围仅限于经审批的业务合作场景下的使用目的，且限定于最小、必要的范围。数据接收（使用）方违法或违约使用、披露数据提供方数据时，数据提供方有权终止本合同、停止数据服务并要求数据接收（使用）方承担责任、赔偿损失。

3.4 数据接收（使用）方将接收的数据提供给第三方时，应获取数据提供方的书面同意，同时遵循本协议第二条关于数据提供方的义务条款。

3.5 数据接收（使用）方不得利用工作过程中知悉的各领域数据资产、所涉及的系统平台、关联的数据处理设备及客户隐私、网络与业务运营中产生的数据，包括客户信息（个人客户信息、集团客户信息）、网络运维数据、业务支撑数据、业务平台数据、技术规范、配置数据与拓扑、项目管理信息、源代码等资料等为本企业或外部合作单位或任何个人谋取利益，禁止将数据上传至任何互联网分享平台(如百度文库、Gitee、Github 等)。

3.6 数据接收（使用）方作为数据处理者，应承担数据安全管理的主体责任。数据接收（使用）方同意建立有效的安全管理制度及应急响应机制，采取有效的技术防护措施保护数据提供方数据，以防止数据被非授权访问或越权访问，防止数据泄漏，并有效保障相关数据资产、系统设备的安全，该保护措施应合理并不低于数据提供方保护自身数据所采取的保护措施。如数据接收（使用）方在数据处理过程中无法提供足够的安全保护水平或发生安全事件的，应及时通知数据提供方。数据接收（使用）方应当针对接触敏感数据的员工签订《数据安全责任承诺书》，明确个人安全保密义务和责任并开展相关安全培训宣教。数据接收（使用）方对于其处理数据期间发生的被盗、泄露或其他有损数据提供方数据安全性的事件承担全部责任，因此造成数据提供方损失的，数据接收（使用）方应负责赔偿，并负责消除社会不良影响。数据接收（使用）方违反适用法律法规、数据提供方各项网络信息安全和数据安全管理相关制度或规范以及本合同约定使用数据，损害数据主体或任何第三方权益的，由数据接收（使用）方承担全部责任。

3.7 如涉及个人信息处理，数据接收（使用）方应当协助数据提供方响应个人主体的权利请求，记录相关处理活动，协助完成个人信息保护影响评估。

3.8 若依法律规定或司法机关、监管部门要求数据接收（使用）方或数据提供方披露数据的，收到监管要求方需予以配合并在合法的范围内应事先通知另一方；双方应对数据采取必要安全措施，或要求披露该数据的司法机关或监管部门提供书面确认，以确保该司法机关或监管部门对该被要求披露的数据采取法律要求的最高级别的保护。本款所述情况发生后，收到监管要求方未及时有效通知数据提供方致使未能采取必要保护措施的，受损方有权要求其承担因数据披露、扩散造成的所有损失。

3.9 数据接收（使用）方只限于将上述数据提供给本单位确有知悉必要的参与数据操作和管理的实施数据操作与管理人员或者运维工程师等，不得将保密数据向任何与实现对接无关的其他人员提供；数据接收（使用）方应确保参与数据操作和管理的数据接收（使用）方人员严格遵守本协议所规定之保密义务，如果数据操作人员有违反本协议规定的情况，即视为数据接收（使用）方之违约行为，数据提供方有权追究数据接收（使用）方相应法律责任。

3.10 数据进入数据接收（使用）方所辖网络环境后，数据接收（使用）方需严格做好系统安全测评和网络安全加固，在存储数据信息的系统受到网络攻击时能够采取必要措施、技术手段进行有效防护，包括但不限于：数据模糊化、传输加密、终端管控、账号和日志审计等技术管控措施。如该系统因遭遇网络入侵、非法使用等原因造成数据提供方提供的数据泄露，数据接收（使用）方需承担违约责任，并且承担相应的法律后果和法律责任。

3.11 如有违反或可能违反本协议的情形发生，数据接收（使用）方应立即通知数据提供方，以便于数据提供方尽早知情尽早做出预防，降低数据安全风险，以及尽可能减少因为数据安全事故而造成的相应损失和负面影响。

3.12 当甲方作为数据接收（使用）方时，甲方应在乙方要求交回、删除数据或者合作项目结束后的合理期间内按照乙方的要求交回、删除数据以及所有描述和概括该保密数据的文件资料及有关数据载体，不能擅自处理，并向乙方提供已删除证明。法律法规另有规定的情形除外。

3.13 当乙方作为数据接收（使用）方时，乙方应在甲方要求交回、删除数据或者合作项目结束后的合理期间内按照甲方的要求交回、删除数据以及所有描述和概括该保密数据的文件资料及有关数据载体，不能擅自处理，并向甲方提供已删除证明。法律法规另有规定的情形除外。

3.14 数据接收（使用）方应采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施和其他必要措施，确保数据的安全性和保密性。

第四条 双方共同的数据安全义务

4.1 双方一致认可业务合作中数据安全的重要性。双方在业务合作中披露、提供、交付给对方的数据，包括但不限于以书面、口头或电子的形式提供的数据，应依法履行相应的数据安全义务及保护数据主体合法权益。

4.2 双方一致确认，在符合适用法律法规并满足各项网络信息安全和数据安全管理相关制度或规范要求的前提下，各项业务合作中的数据使用均应坚持目的特定原则、最小够用原则，以及端到端安全管控和分级管控原则。各方均应建立端到端的数据安全管控制度及事后的审计和合规性审查制度并积极实施。

4.3 双方一致确认，须建立合作数据安全风险监督管理机制，合作期内每年至少开展一次合作数据使用情况抽查，对合作数据安全风险开展动态评估。

4.4 双方保证仅为履行项目合作的目的向各自确有知悉必要的雇员、股东、董事、顾问和/或咨询人员披露数据。在上述人员知悉该数据前，应向其说明数据的保密性及其应承担的义务，开展数据安全和保密教育，保证上述人员同意接受本协议条款的约束，并对上述人员的数据安全和保密行为进行有效的监督管理。

4.5 双方承诺，任何一方不得非法收集、存储、使用、加工、传输、提供、公开、删除、出售本协议项下涉及的个人信息及其他数据，不得违反法律法规的相关规定以及本协议的相关约定。

4.6 涉及重要数据处理时的双方的义务

4.6.1 涉及重要数据处理时，双方应当明确数据安全负责人和管理机构，落实数据安全保护责任。

4.6.2 双方应当按照规定对各自的重要数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

4.6.3 双方应对涉及的重要数据采取备份和加密等法律法规要求的措施。

4.6.4 涉及关系国家安全、国民经济命脉、重要民生、重大公共利益的国家核心数据处理时，双方应按照法律法规的要求，实行更加严格的管理制度和保护措施。

4.7 双方应当加强风险监测，发现数据安全缺陷、漏洞、泄露等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施并依照法律法规要求向数据提供方或数据主体和监管部门履行报告义务。

4.8 双方应就具体的数据处理场景，另行通过签署具体业务合作协议等双方共同认可的方式明确数据提供的范围、类别、条件和程序。具体业务合作协议与本协议存在冲突的，以具体业务合作协议为准。

第五条 转让限制

未经对方事先书面同意，任一方不得将本协议的部分或全部或者本协议项下的任何权利或义务让与或转让给任何第三方。

第六条 不可抗力

任何一方遭遇不可抗力而耽搁或妨碍其履行本协议不视为违约，不须承担因此给对方造成的损失。不可抗力包括但不限于自然灾害、政府行为、许可地区信息产业主管政府部门的命令、电信运营商导致的原因、立法的变化、火灾、水灾、爆炸等。发生不可抗力时双方应当在能力范围内采取措施防止损失进一步扩大。如果此因上述情形耽搁或妨碍履约持续 30 日，一方经书面通知并经双方一致同意后可终止本协议。

第七条 违约责任

7.1 一方未履行或未完全履行本协议下的条款将构成违约，除应当支付违约金外，违约方应赔偿其违约行为给守约方造成的全部损失。包括且不限于守约方因此受到的直接、间接、连带、特殊损失，以及守约方为调查违约方违约所支付的费用和因违约方违反本协议而导致的任何支出、罚金和费用等。如乙方违反本协议的，甲方有权利采取将乙方纳入甲方合作负面行为名单，将乙方纳入行业负面行为名单等措施。

7.2 双方职员违背承诺的，未按照本协议规定使用数据信息，或未遵守数据安全管理规定造成信息泄露，或向除甲乙双方外的第三方披露数据及客户信息，或依据本合作项目的数据信息向第三方做出任何建议，或利用本合作项目的数据信息进行新的研究开发，均视为违反本承诺。

7.3 数据接收（使用）方违反本协议规定的，应立即停止违反本协议的行为，及时采取补救措施防止数据信息泄露范围继续扩大，并向数据提供方支付违约金，违约金的总额不超过业务合作费用总额的【20%】。如果因此导致数据提供方的竞争对手知悉数据提供方的商业秘密和其他秘密，或因此而给数据提供方造成重大经济损失和其他严重不良影响的，违约金金额增加为合同总额的【100%】，数据提供方有权终止与数据接收（使用）方之合作。

第八条 协议终止与解除

8.1 经甲乙双方协商一致，可以变更或提前终止本协议。

8.2 一方出现严重违反本协议约定的行为，另一方可以随时解除本协议，并有权要求违约方承担相应违约责任，赔偿相应损失。

8.3 因不可抗力因素致使无法实现合同目的，任何一方可以解除本协议。

8.4 协议期限内，一方依法破产、解散、撤销或者因其他原因撤销主体资格的，另一方可视为本协议终止。

8.5 双方业务合作终止后【5】年内，数据提供方有权对数据接收（使用）方数据销毁情况进行不定期抽查，如发现数据接收（使用）方超期留存数据的，数据接收（使用）方应当立即删除数据，并向数据提供方支付业务合作费用总额【20%】的违约金。

第九条 信息保密责任及知识产权

9.1 本协议任何一方应对本协议所涉及的任何内容以及双方在执行本协议过程中相关的一切法律、商业、合作业务的所有资讯进行保密。未经对方允许或法律强制性规定外，均不得向各方以外的任意第三方披露。

9.2 除双方另有约定外，甲方提供的数据产品的著作权、专利权及其他知识产权均归甲方及甲方关联方所有。未经明确授权，乙方不得更改、演绎、拆分、反解甲方的技术和程序或以其它任何方式进行可能损害甲方专有权利的行为。

9.3 数据信息的保密责任期限为自本协议生效之日起至数据信息失去其保密性质并为公众所知悉之时为止，不因“合作”终止或解除（协议有效期届满）而结束。

第十条 法律适用和争议解决

本协议适用中华人民共和国法律。所有因本协议引起或与本协议有关的任何争议将通过双方友好协商解决。如经协商不能达成协议解决，则任何一方均有权

按照《互联网数据中心业务协议》中双方约定的争议解决方式向相关争议解决机构提出争议解决诉求。

第十一条 补充协议及附件

双方同意，在本协议签订后，如另有补充协议，该补充协议及附件共同构成本协议不可分割的组成部分，具有同等法律效力。

第十二条 协议生效及其他

12.1 本协议经甲乙双方授权代表签字并加盖公章或合同章后之日起生效，所涉及的数据合作期限与本合同保持一致。

12.2 本协议一式肆份，甲乙双方各执贰份，具有同等法律效力。

12.3 如果本协议的任何条款在任何时候被认定为不合法、无效或不可强制执行而不从根本上影响本协议的效力时，本协议的其它条款不受影响。

12.4 对本协议内容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协议的不可分割的部分。

甲方：【梧州市公安局】（盖章）

甲方法定代表人或授权代表（签字）：【　　】

日期：【2025.11.3】

乙方：【中国移动通信集团广西有限公司梧州分公司】（盖章）

乙方法定代表人或授权代表（签字）：【　　】

日期：【2025.11.1】

附件七：商务需求响应表、服务需求响应表

4. 商务条款偏离表

商务条款偏离表

项目名称：梧州市公安局天网后端设备机房租赁托管服务采购项目

项目编号：WZZC2025-G3-990237-GXXK

所投分标（此处有分标时填写具体分标号，无分标时填写“无”）：__无__

项号	招标文件的商务条款	投标文件响应的商务条款	偏离说明
一	（一）交付使用时间及地点：1、合同签订期：自成交通知书发出之日起15日内，完成签订合同。网络数据链路服务和属于梧州市公安局的托管机柜租赁服务由梧州市公安局与中标供应商签订服务合同，属于梧州市公安局交通警察支队的托管机柜租赁服务由梧州市公安局交通警察支队与中标供应商签订服务合同，并分别按合同内容和考评结果支付合同款给中标供应商。	我公司承诺： （一）交付使用时间及地点： 1、合同签订期：自成交通知书发出之日起15日内，完成签订合同。网络数据链路服务和属于梧州市公安局的托管机柜租赁服务由梧州市公安局与我公司签订服务合同，属于梧州市公安局交通警察支队的托管机柜租赁服务由梧州市公安局交通警察支队与我公司签订服务合同，并分别按合同内容和考评结果支付合同款给我公司。	无偏离
	2、交付使用时间：自签订合同之日起30日内，完成本次租赁服务中所有涉及的机房租用、网络数据链路、机柜提供等部署工作（如果供应商需要将现有天网后端设备搬迁至新的机房运行，供应商负责在合同签订之日起30日内完成天网设备在新机房中的运行环境构建和调试，确保原有设备在拆除、搬迁及安装过程中安全无损。采购人除托管租赁服务费用外，不再因机房的整体搬迁、割接、布线、组网等工程支付额外的费用，搬迁工作须在24小时内完成并恢复所有天网设备正常运行），经采购单位验收确认后，完成交付进入服务期。如中标方无法按时交付使用，采购人有权选择终止合同向中标方追索超期时间段的天网后端设备租赁支出。	2、交付使用时间：自签订合同之日起10日内，完成本次租赁服务中所有涉及的机房租用、网络数据链路、机柜提供等部署工作（如果我公司需要将现有天网后端设备搬迁至新的机房运行，我公司负责在合同签订之日起30日内完成天网设备在新机房中的运行环境构建和调试，确保原有设备在拆除、搬迁及安装过程中安全无损。采购人除托管租赁服务费用外，不再因机房的整体搬迁、割接、布线、组网等工程支付额外的费用，搬迁工作须在24小时内完成并恢复所有天网设备正常运行），经采购单位验收确认后，完成交付进入服务期。如我公司无法按时交付使用，采购人有权选择终止合同向我公司追索超期时间段的天网后端设备租赁支出。	正偏离

	3、合同履行期限：服务期2年（服务期生效时间：所有托管设备部署完成并运行正常，自采购单位验收合格之日起开始计算服务期）。	3、合同履行期限：服务期2年（服务期生效时间：所有托管设备部署完成并运行正常，自采购单位验收合格之日起开始计算服务期）。	无偏离
	4、交付地点：广西梧州市采购人指定地点。	4、交付地点：广西梧州市采购人指定地点。	无偏离
二	（二）结算及付款方式：1、本项目无预付款。	我公司承诺：（二）结算及付款方式：1、本项目无预付款。	无偏离
	2、在服务期内采购人每3个月对服务考评一次（考评标准详见第五章拟签订的合同文本 第六条服务考评），每半年按考评结果向中标供应商结算一次费用，其中：托管租赁费用按实际使用的机柜数量结算；梧州市公安局天网后端设备托管网络数据链路服务费用按使用月份数量结算。中标供应商向采购单位开出对应金额有效的增值税发票，采购单位收到发票后向中标供应商付清本次结算费用（不计利息）。	2、在服务期内采购人每3个月对服务考评一次（考评标准详见第五章拟签订的合同文本 第六条服务考评），每半年按考评结果向中标供应商结算一次费用，其中：托管租赁费用按实际使用的机柜数量结算；梧州市公安局天网后端设备托管网络数据链路服务费用按使用月份数量结算。我公司向采购单位开出对应金额有效的增值税发票，采购单位收到发票后向我公司付清本次结算费用（不计利息）。	无偏离
	备注：如机柜投入使用数量未达到70个，托管租赁费用按实际使用的机柜数量结算，机柜的租费以机柜投入使用月份开始计费（例如在2025年9月内新增2个机柜投入使用，这2个机柜的租费就在2025年9月起开始计费）。 当机柜投入使用数量达到70个后，为保证甲乙双方的合法权益，双方根据项目实际情况核实并调整。任何对本合同的补充、修改或变更，均须以书面形式经双方签署生效。但补充协议涉及合同总金额增减超过原合同金额10%（或其他比例）的，则需按《中华人民共和国政府采购法》的程序执行。	备注：如机柜投入使用数量未达到70个，托管租赁费用按实际使用的机柜数量结算，机柜的租费以机柜投入使用月份开始计费（例如在2025年9月内新增2个机柜投入使用，这2个机柜的租费就在2025年9月起开始计费）。 当机柜投入使用数量达到70个后，为保证甲乙双方的合法权益，双方根据项目实际情况核实并调整。任何对本合同的补充、修改或变更，均须以书面形式经双方签署生效。但补充协议涉及合同总金额增减超过原合同金额10%（或其他比例）的，则按《中华人民共和国政府采购法》的程序执行。	无偏离
三	（三）投入项目人员 本项目至少须提供1名项目经理，5名项目实施人员，3名售后人员。 注：需提供人员的计算机或通信或电气等相关专业的大专及以上学历证书或职称证书或岗位证书等。	我公司承诺： （三）投入项目人员 本项目提供1名项目经理，5名项目实施人员，4名售后人员。 我公司已经提供相关人员的证书证明，详见技术文件2.4.2.4 人员配置明确	无偏离

四	（四）售后服务要求：1、提供全年365*24小时的不间断故障申报服务，故障申告响应时间为30分钟，故障处理人员在接到报告后8个小时内负责排除故障，直到网络恢复正常，如因网络故障在24小时内无法解决的必须提供替代解决方案。	我公司承诺：（四）售后服务要求：1、提供全年365×24小时的不间断故障申报服务，故障申告响应时间为20分钟，故障处理人员在接到报告后7个小时内负责排除故障，直到网络恢复正常，如因网络故障在24小时内无法解决的提供替代解决方案。	正偏离
	2、因本项目的特殊性，供应商如非梧州本地的，供应商必须在响应文件中承诺成交后在梧州市内设有本地化维护服务机构和本地化维护人员及维护设备。	2、因本项目的特殊性，我公司如非梧州本地的，我公司在响应文件中承诺成交后在梧州市内设有本地化维护服务机构和本地化维护人员及维护设备。（详见技术文件3.3在梧州本地内有售后服务机构或承诺成交后设立，提供服务电话）	无偏离
	3、提供免费定期回访以及巡检服务；	3、提供免费定期回访以及巡检服务；	无偏离
	4、提供每周7×24小时技术支持服务。	4、提供每周7×24小时技术支持服务。	无偏离
	5、供应商须提供针对本项目有效的联系人列表（运营商客户经理和技术接口人及联系电话清单）	5、我公司提供针对本项目有效的联系人列表（详见3.3在梧州本地内有售后服务机构或承诺成交后设立，提供服务电话）	无偏离
五	（五）验收标准及要求：1、行业的国家标准、行业标准、地方标准或者其他标准、规范。	我公司承诺：（五）验收标准及要求：1、行业的国家标准、行业标准、地方标准或者其他标准、规范。	无偏离
	2、采购方将按相关行业标准对服务中所有涉及的机房租用、网络数据链路、机柜进行交付使用前阶段性验收，验收通过后才正式进入服务期。阶段性验收合格后由采购方和中标方签署验收单并加盖双方公章，双方各执一份。	2、采购方将按相关行业标准对服务中所有涉及的机房租用、网络数据链路、机柜进行交付使用前阶段性验收，验收通过后才正式进入服务期。阶段性验收合格后由采购方和我公司签署验收单并加盖双方公章，双方各执一份。	无偏离
	3、阶段性验收过程中所产生的一切费用均由供应商承担。报价时应考虑相关费用。	3、阶段性验收过程中所产生的一切费用均由我公司承担。报价时考虑相关费用。	无偏离
	4、在服务过程中，采购方每3个月对中标方考评一次。	4、在服务过程中，采购方每3个月对中标方考评一次。	无偏离
六	（六）报价要求：投标报价应包括供应商提供本项目服务内容、托管设备搬迁（如有）、所需场所、工具、安装、调试、验收、培训、电费、服务人员等各种费用、售后服务、税金及其它不可预见等一切费用。单项报价不能超过单价上限控	我公司承诺：（六）报价要求：投标报价包括我公司提供本项目服务内容、托管设备搬迁（如有）、所需场所、工具、安装、调试、验收、培训、电费、服务人员等各种费用、售后服务、税金及其它不可预见等一切费用。单项报价不能	无偏离

	制价，否则作无效报价处理。	超过单价上限控制价，否则作无效报价处理。	
七	（七）应急保障：1、紧急故障情况下的专用流程 （1）技术要求：中标人应 7*24 驻守机房值班室，当采购人的设备出现紧急故障，需要立即进入机房现场处理故障，中标人应提供必要的专用流程协助采购人已授权人员顺利进入本次租赁的大楼和机房，并做好设备故障进行分析、处理，制定故障解决方案，编制故障分析及处置报告。	我公司承诺： （七）应急保障： 1、紧急故障情况下的专用流程 （1）技术要求：我公司提供 7*24 驻守机房值班室，当采购人的设备出现紧急故障，需要立即进入机房现场处理故障，我公司提供必要的专用流程协助采购人已授权人员顺利进入本次租赁的大楼和机房，并做好设备故障进行分析、处理，制定故障解决方案，编制故障分析及处置报告。	无偏离
	（2）维护要求：提供《紧急故障处理进出机房专用流程》文档，并负责落实流程的实施。	（2）维护要求响应：提供《紧急故障处理进出机房专用流程》文档，并负责落实流程的实施。	无偏离
	2、应急演练 按采购人要求提供但不限于电力、空调、消防、视频监控等应急预案，并按采购人要求每半年开展一次应急演练。	2、应急演练 按采购人要求提供但不限于电力、空调、消防、视频监控等应急预案，并按采购人要求每半年开展一次应急演练。	无偏离

注：

1. 表格内容均需按要求填写并加盖投标人公章。

2. 请逐条对应本项目招标文件“第二章　采购需求”中“商务条款”的要求，详细填写相应的具体内容。“偏离说明”一栏应当选择“正偏离”或“负偏离”或“无偏离”进行填写。

3. 当投标文件的商务内容低于招标文件要求时，投标人应当如实写明“负偏离”。

投标人名称(盖公章)：中国移动通信集团广西有限公司梧州分公司

日期：2025 年 10 月 24 日

1. 服务要求偏离表

服务要求偏离表

项目名称：梧州市公安局天网后端设备机房租赁托管服务采购项目

项目编号：WZZC2025-G3-990237-GXXK

所投分标（此处有分标时填写具体分标号，无分标时填写“无”）：无

项号	标的名称	招标文件采购需求中的服务内容	投标文件响应的服务内容	偏离说明
1	机柜租用托管服务（含机房搬迁）	机房租赁服务 要求提供 70 个机柜租赁服务，租用期 2 年，其中市局在用 45 柜，备用 [illegible] 柜；交警在用 11 柜，备用 5 柜。单机柜空间≥44U（可完全利用），单机柜设计功耗≥4 千瓦，满足 TIER 3 保障级别。	我公司承诺： 机房租赁服务 提供 70 个机柜租赁服务，租用期 2 年，其中市局在用 45 柜，备用 [illegible] 柜；交警在用 11 柜，备用 5 柜。单机柜空间 44U（可完全利用），单机柜设计功耗 4 千瓦，满足 TIER 3 保障级别。	无偏离
		1、项目整体要求 提供 1 项天网后端设备机房租赁托管服务；服务期 2 年。	1、项目整体要求 提供 1 项天网后端设备机房租赁托管服务；服务期 2 年。	无偏离
		2、机房基础设施要求 数据中心机房要求具备机柜的托管能力≥100 个，以便于后期机柜需求的扩容，单机柜空间≥44U（可完全利用），单机柜设计功耗≥4 千瓦，满足 TIER 3 保障级别。要求采用密闭冷通道模块化机房的机柜部署方式。 数据中心要求设有卸货平台、货运电梯（机房不在地层需提供）、高压配电室、UPS 室&电池间、维护工作间等设施。	2、机房基础设施要求 数据中心机房具备机柜的托管能力 300 个，以便于后期机柜需求的扩容，单机柜空间 44U（可完全利用），单机柜设计功耗 4 千瓦，满足 TIER 3 保障级别。采用密闭冷通道模块化机房的机柜部署方式。 数据中心设有卸货平台、货运电梯（机房不在地层需提供）、高压配电室、UPS 室&电池间、维护工作间等设施。	无偏离

		3、机房电力配置 电力供应系统满足≥2路高压市电接入要求；具备不低于2套UPS不间断电源，每套UPS负载能力不低于400KVA，设计系统满载情况下UPS后备时间不低于15分钟；配备不低于2套功率400KW柴油发电机系统。	3、机房电力配置 电力供系统满足2路高压市电接入要求；具备3套UPS不间断电源，每套UPS负载能力400KVA，设计系统满载情况下UPS后备时间15分钟；配备2套功率2000KW柴油发电机系统。	正偏离
		4、机房制冷系统 机房冷通道配置专用列间精密空调，并要求按（N+X（X≥1））的冗余标准配置。	4、机房制冷系统 机房冷通道配置专用列间精密空调，并按（N+X（X≥1））的冗余标准配置。	无偏离
		5、机房消防系统 要求机房配置火灾自动报警系统、消防联动控制系统、火灾应急广播系统、防排烟系统及灭火控制系统等；消防系统需采用七氟丙烷灭火装置及设备，结合极早期烟雾探测系统及温感、烟感双路感应，可实现定点报警并处置。	5、机房消防系统 要求机房配置火灾自动报警系统、消防联动控制系统、火灾应急广播系统、防排烟系统及灭火控制系统等；消防系统采用七氟丙烷灭火装置及设备，结合极早期烟雾探测系统及温感、烟感双路感应，可实现定点报警并处置。	无偏离
		6、机房网络引入 提供运营商网络到托管设备之间的交换数通配置服务。在机房外预留不少于一处外接光交箱，有足够纤芯引入到机房内，方便各家天网系统线路运营商接入资源使用。机房内提供良好的网络布线条件，便于搭建安全、可靠的专用数据通道环境，从而满足天网平台点到点、点到多点的访问需求。	6、机房网络引入 提供运营商网络到托管设备之间的交换数通配置服务。在机房外预留一处外接光交箱，有足够纤芯引入到机房内，方便各家天网系统线路运营商接入资源使用。机房内提供良好的网络布线条件，便于搭建安全、可靠的专用数据通道环境，从而满足天网平台点到点、点到多点的访问需求。	无偏离
		7、用电量计费 服务供应商承担所有托管设备的用电费用（包括机房环境保障等用电）。	7、用电量计费 我公司承担所有托管设备的用电费用（包括机房环境保障等用电）。	无偏离
		8、机房维护能力 要求提供机房专业运维团队，提供全方位基础运维服务，含维护、变更、容量管理等方面内容，并有专人7*24小时轮班值守，提供天网平台保障人员进行维护的	8、机房维护能力 我公司提供机房专业运维团队，提供全方位基础运维服务，含维护、变更、容量管理等方面内容，并有专人7*24小时轮班值守，提供天网平台保障人员进行维护的便利条件。	无偏离

		便利条件。		
2	网络数据链路服务	1、提供1条（两端地址：托管机房至梧州市公安局负一层机房）专线电路，线路带宽≥3000Mbps，速率上下行对等，服务期为2年；	我公司承诺：1、提供1条（两端地址：托管机房至梧州市公安局负一层机房）专线电路，线路带宽3000Mbps，速率上下行对等，服务期为2年；	无偏离
		2、传输技术要求采用波分技术，提供点对点的透明承载，业务端两端物理接口为万兆光口；	2、传输技术采用波分技术，提供点对点的透明承载，业务端两端物理接口为万兆光口；	无偏离
		3、传输骨干网具有故障自动倒换功能，能保证电路不会因光缆的意外阻断和部分设备的故障而中断；	3、传输骨干网具有故障自动倒换功能，能保证电路不会因光缆的意外阻断和部分设备的故障而中断；	无偏离
		4、传输设备要求具有全网网管监控功能，并实行7*24小时实时监控，具备可靠网管系统；	4、传输设备要求具有全网网管监控功能，并实行7*24小时实时监控，具备可靠网管系统；	无偏离
		5、网络性能要求：端到端电路平均网络延时≤10ms；端到端电路丢包率≤0.1%。	5、网络性能要求：端到端电路平均网络延时10ms；端到端电路丢包率0.1%。	无偏离

注：

1.表格内容均需按要求填写并加盖投标人公章。

2.请根据所投服务内容，逐条对应本项目招标文件“第二章 采购需求”中“服务要求”的服务内容作出明确响应，并作出偏离说明。“偏离说明”一栏应当选择“正偏离”或“负偏离”或“无偏离”进行填写。

3.当投标文件的服务内容低于招标文件要求时，投标人应当如实写明“负偏离”。

投标人名称(盖公章)：中国移动通信集团广西有限公司梧州分公司

日期：2025年10月[illegible]日