合同编号：

2023省工业和信息化厅网络安全维护项目运维服务合同

甲　　方：贵州省工业和信息化厅

乙　　方：联通数字科技有限公司贵州省分公司

签订时间：2024年 1月 25日

签订地点：贵州省贵阳市云岩区

本合同由以下双方共同签署：

甲　　方：贵州省工业和信息化厅

法定代表人：敖鸿

通信地址：贵州省贵阳市中华北路 185 号

邮政编码：550000

纳税人识别号：11520000MB0U07242Q

联 系 人：郑浩

联系电话：085188668155

乙　　方：联通数字科技有限公司贵州省分公司

法定代表人：蒯芳

通信地址：贵州省贵安新区黔中路电子信息产业园内

邮政编码：550000

开户名称：联通数字科技有限公司贵州省分公司

开户银行：中国工商银行股份有限公司贵阳万东支行

账　　号：2402004919200125779

纳税人识别号：91520900337342524F

联 系 人：徐丽

联系电话：18685192087

传　　真：/

【注：本合同双方的账户名称、开户银行、银行账号以本合同提供的为准，如有变更，变更一方应在距合同约定的相关付款期限届满二十五天前，以加盖财务专用章的书面文件通知另一方；否则视为变更无效，一切不利后果由变更方自行承担。】

甲乙双方遵照《中华人民共和国民法典》及有关法律、行政法规，本着诚实信用、平等双赢、长期合作、共同发展的原则，经友好协商一致，就2023省工业和信息化厅网络安全维护项目签订本合同，以兹共同信守。

一、词语定义

下列名词和用语，除上下文另有规定外，有如下含义：

1．项目：是指甲方委托乙方进行运维服务的项目。

2．甲方：是指承担直接投资责任和委托运维服务的一方及其合法继承人。

3．乙方：是指承担运维服务业务的一方及其合法继承人。

4．工作日：是指除国家法定节假日和休息日以外的日期。

5．7*24小时：每周7天，每天24小时。

6．资产清单：是指由甲方或最终用户拥有或控制的资产明细表。

7．设备物料清单：是指产品所需零部件明细表、软件产品构成明细表及其产品结构等。

二、项目背景

（一）项目名称

2023省工业和信息化厅网络安全维护项目

（二）项目概述

2023省工业和信息化厅网络安全维护项目主要采用远程+驻场服务方式运维。主要包含以下内容：

1．运维内容：漏洞扫描、安全基线核查和加固服务、渗透测试服务、风险评估服务、网络分析与优化服务、安全策略管理服务、应急响应服务、应急演练服务、备品备件等。

2．运维指标：提供5×8小时运维服务及7×24小时电话服务，响应时间不得超过半小时，如需现场处理4小时内到达现场；重大事项及活动期间需提供24小时保障服务。

3．服务方式:采用远程+驻场服务方式，驻场1人，具备本科学历、计算机专业，满足网络安全服务需求。

4．服务期限：12个月（2023年4月1日至2024年3月31日）。

（三）最终用户

贵州省工业和信息化厅

三、项目类型

信息安全类，技术服务支撑类

四、服务内容

（一）信息安全类服务内容

乙方向甲方提供贵州2023省工业和信息化厅网络安全维护项目运维保障服务，服务内容主要包括漏洞扫描、安全基线核查和加固服务、渗透测试服务、风险评估服务、网络分析与优化服务、安全策略管理服务、应急响应服务、应急演练服务、备品备件等。

（二）技术服务支撑类服务内容

乙方向甲方提供贵州2023省工业和信息化厅网络安全维护项目运维保障服务，服务内容主要包括漏洞扫描、安全基线核查和加固服务、渗透测试服务、风险评估服务、网络分析与优化服务、安全策略管理服务、应急响应服务、应急演练服务、备品备件等，提供1人，在贵州省工业和信息化厅场所提供支撑服务。

五、服务期限

乙方应在12个月服务期内开展运维服务。乙方应严格按进度计划要求执行，如因乙方原因而造成运维工作延误，则乙方应承担由此造成的相应责任和损失。

六、服务要求

1．乙方应保证指派经验丰富的运维负责人苏雄（身份证号：522422199612052050，联系电话：18685190906）为本运维项目的专职负责人，负责项目的沟通和协调工作。

2．如果甲方认为乙方指派的运维项目负责人不能胜任的，乙方应当在【15】个工作日内及时更换。

3．乙方应保证服务人员相对固定，如有变动，乙方应至少提前【1】个月以书面形式通知甲方，并征得甲方书面同意。

4．乙方指派的项目负责人和运维服务人员需实际参与本合同项目的运维服务工作。

5．乙方需在本合同签订前向甲方提供完整、专业的运维服务流程和团队组织架构，并明确项目成员岗位和工作职责。

6．乙方需建立运维服务相关的人员培养机制和人员储备计划，确保项目人员能够满足甲方以及最终用户方的运维服务需求。

7．乙方需建立运维服务相关的绩效考核机制，定期对运维服务人员进行全方位的运维服务质量考核。

七、考核标准

甲方将以考核的方式确定乙方的运维保障服务质量是否达到要求，并根据考核结果确定最终付款比例。考核标准详见附件 1《项目运维服务管理规范》和附件 2《网络及数据安全管理要求》。

八、合同金额及付款方式

1．甲乙双方间发生的一切费用均以人民币结算支付，合同款项由甲方以转账、电汇支付至乙方在本合同封二指定的账户，合同款项均为无息支付。

2．本项目合同总金额:【￥525,000.00 】元整（大写:【伍拾贰万伍仟】元整），该费用为含税价，税率为【6%】。费用包含：完整的运维交付成果、技术文件费用、乙方应承担提供技术服务和技术支持的费用、技术培训费用（包括教材、课程费等），以及乙方为全面履行合同义务所需支付的所有其他费用。

3．付款方式:

根据项目资金情况，按以下条款等比例地支付合同款项。

（1）合同签订后，甲方收到乙方提供的《付款申请》和等额增值税专用发票后【90】个工作日内，支付乙方【100%】。

4．甲方收到乙方开具合法等额增值税专用发票后，按照本合同条款约定支付相应款项；因乙方出具的发票存在类型、金额、合法性等问题导致甲方延期付款的，甲方不承担逾期付款的违约责任。

5．在合同履行期间，如遇国家政策调整等因素，导致所开具发票的税率与上述约定不一致，则合同总金额相应调整。

6．由于乙方未足额缴纳应缴税款和开具发票不真实、不合格而引起的一切责任（包括商业责任和法律责任）和损失，由乙方全部承担。由此给甲方造成的所有损失，乙方还应予全额赔偿。

九、项目验收

乙方根据甲方的书面运维需求完成运维服务后，应按照合同及附件约定的内容进行成果交付，乙方在交付前应按本合同的要求进行内部自检，自检通过后通知甲方，所交付的文件应当是电子版和纸质版文档。乙方在交付前【15】个工作日内以书面方式或电子邮件形式通知甲方，乙方将运维成果交付甲方后，甲方应在【10】个工作日内组织验收。

1. 验收标准：本项目采用现场/远程验收方式验收，验收标准以符合招标（采购）文件、投标（应答）文件、合同相关附件所列明的服务和甲方的要求为准。乙方所提供的服务应符合本合同条款中所述的标准；如果没有列明适用标准，则应符合中华人民共和国国家标准或行业标准；如果中华人民共和国没有相关标准的，则采用货物来源国适用的官方标准。这些标准必须是有关机构发布的最新版本的标准。乙方应向甲方提供有关标准的中文文本。

2. 验收人员：由【甲乙双方人员】共同参与，甲方最终用户有权聘请第三方专业机构人员参与验收。

3. 项目验收：运维期满后，经乙方内部自查通过，即可按照项目进度配合甲方进行验收。乙方应完成本合同“六、服务要求”所有运维服务内容，所有运维服务成果符合合同要求。同时，乙方须提供验收文档包括但不限于《项目运维月报》《运维考勤表》（涉及人员驻场项目提供）《巡检记录》《问题处理记录》《运维期用户使用意见》《运维服务总结报告》等。

4. 甲方验收不合格，应出具书面的异议。乙方根据甲方要求，应及时加以修改纠正，直至验收合格为止。

5. 所有验收节点必须由甲方共同确认后方可视为验收通过。

十、双方的义务、权利和责任

（一）甲方的义务和权利

1. 义务

（1）负责项目实施内外部关系的协调，为乙方开展运维服务项目实施中的调研、安装、测试等工作提供必要的工作环境条件及协助。

（2）指定项目经理负责与乙方联络和协调，如更换项目经理，应及时书面通知乙方。

（3）在约定的时间内就乙方书面提交并要求做出决定的一切事宜做出书面决定。

（4）需配合乙方对运维服务进行验收，并及时反馈书面修改意见和验收结论性报告。

（5）负责组织相关人员参加由乙方提供的技术培训。

（6）负责协调相关厂商，配合乙方做好调研、施工运维工作和技术对接。

（7）负责落实甲方内部人员的保密安全管理责任。

（8）甲方有权要求乙方工作人员对运维账号及密码进行保密，账户及密码只限本人使用，不得借他人使用。

2. 权利

（1）甲方具有对服务标准、服务流程设计和服务要求的认定权，以及对服务内容变更的审批权。

（2）甲方有权否定任何乙方做出的损害甲方利益的决定和行为，并有权向乙方索赔。

（3）乙方调整其项目小组人员时须经甲方书面同意。

（4）甲方有权要求乙方提交工作报告及合同约定的专项报告。

（5）甲方有权对乙方提供的运维及服务工作内容提出修改意见，确保能够真正满足甲方工作的实际需要。

（6）甲方有权要求乙方更换不称职的人员，若乙方未按照本合同约定及时更换，则甲方有权解除本合同，且乙方应当返还甲方已支付的款项。

（7）甲方有权不接受乙方的意见或建议。如乙方的意见与甲方有分歧，以甲方的最终意见为准，乙方必须执行。甲方对其最终意见的执行结果负责。

（8）甲方有权要求乙方工作人员在规定时间内完成运维服务。甲方在乙方工作人员每一次运维服务完成后，配合检查系统是否正常使用。

（9）甲方有权要求乙方技术负责人或项目负责人每月与甲方指定负责人就运维工作中涉及的相关事宜进行直接面对面沟通，以保证维护工作顺利进行。若因其它原因，无法在约定的时间段内进行面对面沟通工作，则沟通工作转为邮件或电话形式执行。

（10）自合同生效之日起，乙方按照附件 1《项目运维服务管理规范》和附

件2《网络及数据安全管理要求》中的运维内容向甲方提供服务，甲方有权对乙方提供的相关服务质量进行考评，如乙方无法满足本合同条款有关要求，甲方有权减扣或拒绝支付当年服务费。

（二）乙方的义务、权利和责任

1．义务

（1）乙方承诺保证具有并提供实施合同要求的内容所必须具备的资质和资源。

（2）乙方负责根据甲方方的具体需求进行运维服务，并及时与甲方沟通，确保运维服务符合甲方的实际需求。

（3）乙方负责培训甲方方人员，提供相关说明文档。

（4）乙方负责根据甲方方的需求变更，在合同界定的功能范围内适时进行服务的内容调整工作。

（5）乙方应根据甲方的需求，对附件1《项目运维服务管理规范》和附件2《网络及数据安全管理要求》中的运维内容进行运维服务，与本合同具有同等法律效力，本合同与附件不符部分，以附件为准。

（6）乙方保证所提供的各项产品及服务不侵犯任何第三方的合法权益，如发生第三方指控甲方侵权的，由乙方承担全部责任；如甲方因此与第三方发生纠纷，甲方有权对因此产生的所有费用（包括但不限于赔偿金、诉讼费、律师费、公告费、保全费等费用）向乙方追偿。

（7）乙方应严格按照本项目的招标（采购）文件、投标（响应）文件所约定的条款实施本项目，并承诺保证乙方履行合同时符合本合同及本项目的招标（采购）文件、投标（响应）文件，符合国家标准及行业规范，满足甲方方项目运维目标及任务要求，按期、保质完成项目所有运维内容，向甲方完整交付运维服务成果。

（8）甲乙双方参与本项目的工作人员应严格遵循各方安全制度，共同保障各方资料和设备的安全。乙方如需进入机房工作，乙方只能在甲方规定的工作区域对项目涉及的设备进行操作，严禁触动与项目无关的任何设备（包括任何操作行为），如需跨区操作，应得到甲方项目联系人确认。

（9）乙方应提供满足本项目开展的人员配备，包括但不限于：项目经理、

运维人员等。并指定一名固定专业人员作为代表与甲方配合，定期与甲方项目经理对本项目的进度事宜进行沟通，详细了解甲方工作要求，根据甲方工作需要开展运维保障相关工作，及时解决项目运维实施过程中出现的问题。

（10）乙方对甲方的运维项目负责人电话需【24】小时保持开机，随时与甲方保持顺畅的联系方式。

（11）针对未上云（未部署在云上贵州系统平台）的软件系统，乙方应积极配合甲方，进行软件系统上云工作；针对已经上云（部署在云上贵州系统平台）的软件系统，当甲方有平台升级或平台节点迁移需求时，乙方应无条件按照甲方的要求，进行软件系统的迁移工作。

（12）乙方应配合提供甲方申报知识产权所需相关源代码（如有）、资料等。项目验收前【15】日，乙方应向甲方提供完整、准确的项目运维实施及竣工服务资料，包括运维工作记录文件、巡检记录、维护记录、值班记录、运维期用户使用意见、验收报告、运维服务管理报告及运维总结报告等文档，运维工作实施完毕后应汇集成册统一交付给甲方，包括纸质资料和电子版资料。

（13）乙方向甲方书面申请进行项目验收，经甲方方组织的专家组检验确认项目验收合格并签署“项目验收评审结论”后，乙方正式结束运维服务。

（14）合同期内，乙方应根据甲方方信息化总体运维需要，配合甲方和相关厂商做好所承建的系统与相关系统的技术对接。

（15）负责落实乙方及乙方内部人员的保密安全管理责任。

（16）未经甲方书面同意，乙方不得将运维项目工作（包含但不限于调研、服务、改造、升级、安装、测试等）转让、转委托、转包、分包给第三方。

（17）乙方工作人员不得擅自更改运维账号及密码，账号及密码不得借他人使用。

（18）乙方应遵守按双方约定的工作进度完成运维服务工作，每一个阶段的工作完成后应报甲方书面认可方可进行下一阶段的工作。

（19）乙方人员在工作中造成甲方或最终用户财产设备损失的，乙方应当照价进行赔偿。

（20）乙方应严格遵守《网络及数据安全管理要求》，见附件 2。

2．权利

（1）乙方在与甲方签订的合同授权范围内行使合同规定的权利，履行相应的职责。

（2）针对项目有关事项包括项目规模、运维服务标准、业务流程设计和使用功能要求等，具有向甲方提出的建议的权利。

（3）针对本项目服务和其他技术问题，按照安全和优化的原则，具有向甲方的提供建议权，其建议应有技术经济比较。

（4）在任何情况下（包括合同另有规定的情况），凡涉及项目变更、项目增减、议价、索赔、处理事故、改变进度、改变技术标准、改变重大实施方案等及一切有关费用的问题，均应与甲方共同商定，经报甲方批准后方可实施。

（5）组织协调与项目运维实施有关的协作单位，重要协调事项应当事先通知向甲方报告。

（6）未经甲乙双方确认的付款单据，甲方有权拒绝支付。

（7）乙方在项目运维实施过程中，如果有必要的话，可向甲方申请以上未提及的事项的授权，但须征得甲方的书面批准后方能行使。

3．责任

（1）乙方的责任期为合同约定的起始日至项目服务结束日，在项目运维过程中，如遇特殊情况，经双方协商一致后，乙方的责任期也应相应延长。

（2）乙方在责任期内，应承诺必须保证按合同约规定的范围、进度和标准履行合同中约定的义务。如果因乙方过失而造成经济损失，甲方有权要求乙方赔偿。

（3）乙方应保证系统的稳定运行，如出现重大故障应采取及时、准确、适当的补救措施，如因乙方原因造成的损失，乙方将承担由此带来的一切责任。

（4）乙方所有的运维保障工作开展需在甲方同意许可的条件下进行，未经甲方许可，乙方不得对甲方版权所有的系统平台进行任何操作，因此造成的损失，乙方将承担全部责任。

（5）与甲方共同制定和确认每一个阶段的详细工作实施计划（包含运维实施的范围、具体的进度、参加的人员、投入的资源等定义）。

（6）乙方应自备本合同项下必须的人员、办公、通讯、交通等设施、设备，

以及履行本合同所需的所有特殊仪器、工具，并负担所有有关的费用。

（7）乙方应承担其本身及其人员在本合同确指的范围和资格内因错误或疏漏以及严重渎职造成的后果。

（8）乙方在项目调研、运维、开发、安装、测试等运维工作中出现的一切安全责任以及财产损失或人身损害，均由乙方自行负责。

十一、知识产权

1．本合同签署前已存在的著作权、专利权和其他知识产权应属本合同签署之日前已享有该权利的一方所有。

2．因本合同所形成的所有相关成果归甲方所有，甲方是该成果的著作权、专利申请权、专利权、技术秘密及其他一切知识产权的所有人。

3．项目运维过程中产生的所有数据，乙方需要积极配合甲方，按照贵州省统一政府数据接口和数据交换共享标准和要求，实现数据上传数据共享交换平台。乙方未经甲方书面许可，不得将该数据（或以该数据为基础加工产生的数据）用于与合同约定无关的其它用途，因此造成的损失由乙方承担。

4．涉及与项目定制开发有关的技术成果及知识产权归甲方所有，乙方应向甲方提供该项目所有技术成果、建设实施文档、软件源代码和过程数据等。

5．甲方为履行本合同购置的有关设备、器材、资料及其他软件的财产所有权归甲方所有。

6．乙方应保证其提供的产品、工具、模型、方法论、源代码、文档、知识资产及服务没有任何权利瑕疵，没有侵犯任何第三方权利。甲方方在使用该产品或服务的任何一部分时，免受第三方提出的任何侵犯其知识产权的权利主张。如果任何人对甲方方使用该产品及服务主张知识产权权利，由乙方负责处理一切纠纷及相关事宜，由此给甲方方造成的损失，由乙方承担。

7．未经甲方同意，乙方不得以任何方式向第三方披露、转让或许可有关的技术文件、图纸、秘密信息等。除本项目运维工作需要外，未得到甲方书面许可，乙方均不得以任何方式将本项目所涉文件及成果用于商业性质用途。

十二、资料、保密与廉政

1．乙方在与甲方签订合同时，应同时签署《保密协议》（见本合同附件 4），乙方应严格按照相关规定，落实保密措施，确保合作过程中涉及的国家秘密、业

务需求文件、协议、系统设计、技术成果等内容和相关事务的保密安全，未经甲方书面许可，乙方不得向任何第三方提供或透露甲方所有的资料、数据和信息，包括纸质版资料和电子版资料。在本合同期内或合同终止后，未征得有关方同意，不得泄露与本项目、本合同业务活动有关的保密资料。如果乙方或乙方的相关工作人员违反本合同约定的保密义务，乙方应按合同总价的【10%】支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。

2．在项目实施过程中所编纂或准备的报告、全部有关资料以及其它辅助记录或材料将都是甲方的绝对财产，没有甲方事先书面同意，乙方不得将这部分财产以及由甲方提供的有关合同或任何合同条文、规格、计划、图纸、模型、样品或资料提供给乙方雇用于履行本合同以外的任何其他人。即使向本合同的雇员提供，也应注意保密并限于履行合同必须的范围。

3．乙方承诺保证不将甲方提交的资料转让给任何第三方。

4．没有甲方事先书面同意，除了履行本合同之外，乙方不应使用本合同所列举的任何文件和资料。

5．除了合同本身以外，本合同所列举的任何文件均是甲方的财产。如果甲方有要求，乙方在完成合同后应将这些文件（全部拷贝）还给甲方。

6．乙方应根据合同规约定要求向甲方提供所有技术文件。如果工作必需但合同又未作规定的需要乙方才能提供的技术文件，乙方应及时向甲方提供。

7．技术文件应编辑正确，组织合理，内容充实，容易理解。技术文件均应提交甲方确认。乙方应承担甲方完全按照技术文件的指导进行工作导致损失的责任。

8．乙方应按照甲方要求提供技术文件及其电子文件给甲方。技术文件的全部费用已包含在合同价中。

9．甲方应向乙方提供并协助乙方获取履行合同所需的资料和技术文件。

10．在合同生效后【3】年内，甲方和乙方应对相互据合同提供的所有技术文件、报告、费用估算、技术数据和参数予以保密。

11．乙方应对其据合同提供的项目及其任何组成部分的技术文件、报告、资料中出现的矛盾、错误或遗漏负完全责任，甲方对这类文件、报告、资料的确认并不免除乙方的该等责任，除非这类矛盾、错误或遗漏是由于甲方提供的不精确

或错误的资料所致。乙方应自费对此类矛盾、错误和遗漏进行必要的更改和补救工作，并应对相应的文件、图纸、资料进行修改。

12．甲方只须对其以书面方式提交的资料负责。若甲方提供给乙方的资料或文件存在缺陷、遗漏、矛盾或措辞含糊或词意不明或正确性有疑问，则乙方应提请甲方注意。甲方应及时补充或修改。

13．乙方项目实施工作完成后【30】天内必须把所有文件资料（包括技术文件、图纸、证书、函件等）归类整理成册交与甲方。

14．乙方应同时签署《廉洁共建合作协议》（见本合同附件 5），并严格执行，如有违反，经查证属实，将视情节严重程度甲方将对乙方采取警告、取消资格、终止合同、暂停合作等措施；触犯国家法律法规的，移交司法机关处理。

十三、项目培训

1．乙方应向甲方方提供详细的《项目培训计划》，在合同签订之日起至服务期满期间，为甲方指定用户人员及运维人员提供培训。

2．乙方应根据项目实施的计划、进度和需要与甲方的要求，及时安排对甲方指定的相关人员进行培训，培训次数共计【1】次。培训目标为使受训者能够独立、熟练地完成日常管理操作，实现依据本合同所规定的项目建设目标和功能。

3．培训内容包括但不限于以下内容：

对客户培训应急演练内容，完成应急演练工作。对客户的网络安全环境进行事前预防，事中处置，事后溯源。

4．乙方负责培训的人员应具有相应资质及丰富的授课经验，能确保参培人员能快速掌握培训内容，能独立开展工作，并能承担相应的操作使用培训。

5．培训费由乙方承担。乙方需负责提供由于培训中师资所涉及的所有费用。培训地点为甲方或最终用户方所在地或远程。具体培训时间双方协商确定。

十四、合同生效、转包、暂停、续签及终止

（一）合同生效

1．本合同经双方法定代表人或授权代表签字（或盖章）并加盖单位公章后生效。

2．本合同有未尽事宜，必须经甲乙双方共同协商，做出书面补充协议予以确定，补充协议与本合同具有同等的法律效力，补充协议与本合同不一致的，以

补充协议为准。

3．本合同于双方各自履行了合同的全部义务，包括本项目的质保期结束和甲方付清全部合同款后终止。

4．对本合同条款和附件的任何变更、修改或增减，须经双方协商同意后签署书面文件，作为本合同的组成部分并具有同等法律效力。

5．本合同的所有附件及该项目的招标（采购）文件、投标（响应）文件均为本合同不可分割的组成部分，与本合同正文具有同等效力。

（二）合同暂停

1．甲方可以在任何时候由于任何原因书面通知乙方暂停合同的任何部分。乙方应即时暂停，但必须继续执行未暂停的部分，并在收到甲方书面恢复通知后，即时恢复。

2．如并非由于乙方违约导致乙方不得不暂停履行合同或合同一部分时，乙方应立即书面通知甲方，并给出充分合理的解释。乙方必须协助甲方消除影响，以使合同得以继续履行。

（三）合同续签

甲方依据《项目运维服务管理规范》（附件 1）、“九、项目验收”和《网络及数据安全管理要求》（附件 2）对乙方的服务工作进行考核，乙方同时满足下列条件时，甲方可与乙方续签合同。

1．乙方年度服务考核结果评分在【80】分及以上。

2．乙方通过甲方项目验收。

3．乙方网络及数据安全管理考核结果为【优秀】或【一般】或【达标】。

（四）合同终止

1．当服务结束且合同双方完成合同规定的责任和义务，合同自动终止。

2．若双方同意，合同可以在任何条件下终止。这种情况下，双方均无例外地免去对方所有的合同责任和义务。

3．甲方可以在任何时候可以以充足的理由终止本合同，但事先必须在正式终止前【30】天以书面形式通知乙方，并说明终止理由。

4．如因不可抗力导致合同终止，双方均不对对方承担赔偿责任。

5．项目采购、实施过程中，乙方存在下列行为，甲方可单方面终止合同。

（1）乙方有腐败和欺诈行为。为此目的，定义下述条件：

① “腐败行为”是指建议给、给、接受或索要任何价值的东西，以影响甲方职工在与执行合同有关的任何事情上的行为。

② “欺诈行为”是指掩盖事实真相，以不正当的手段影响合同的执行，从而对甲方造成损害，而且包括与其它方面进行勾结，以图获得不公平的好处，进而剥夺甲方正当执行合同的好处。

（2）乙方有泄密行为，经查证属实。

（3）其他行为，严重影响甲方或最终用户工作，给甲方或最终用户造成损失。

6．如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，提出终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

十五、违约责任

1．乙方应保证运维系统稳定运行，若业务中断超过【0.5】小时以上（包含【0.5】小时），乙方未及时发现问题立即响应的，甲方有权要求乙方按照合同总金额【1%】向甲方支付违约金；若业务中断超过【2】小时以上（包含【2】小时），乙方未及时发现问题立即响应的，甲方有权解除合同并要求乙方按总金额【2%】向甲方支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任，承担以上违约责任并不免除乙方协助甲方或涉及到的用户单位解决中断问题的责任。

2．乙方必须按照本合同约定的时间和条件完成运维服务工作，每延期【1】次，甲方有权要求乙方按照合同总金额的【0.5%】向甲方支付违约金；如乙方无故中途解除合同的，乙方必须退回本项目的所有已收款，并按合同总价款的【2%】向甲方支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。

3．如业务需求产生较大的变更、外在不可抗力因素等原因，致使项目期限需要延长的，乙方应及时以书面形式通知甲方，在取得甲方同意的情况下，工期可适度顺延，但累计延期时间不得超过【30】天。

4．发生其它违约情形，违约方应赔偿由此给守约方造成的一切损失。如属双方过错，应各自承担相应责任。因一方违反本合同约定构成违约，另一方提起

诉讼或仲裁维护自身合法权益的，该方有权要求违约方承担由此造成的律师费、诉讼费或仲裁费、保全费、执行费及必要的交通住宿费。该费用的承担不影响违约方承担其他违约责任或损失赔偿责任。

5．如果乙方或乙方的相关工作人员违反本合同约定的保密义务，乙方应按合同总价的【2%】支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。

6．如果乙方违反本合同约定将项目转让、转委托、转包、分包，甲方有权解除合同，并有权要求按合同总价的【2%】支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。

7．乙方的运维管理工作应参照甲方具体指定的维护管理制度及规范进行，包含但不限于运维人员、资产、知识库、服务质量、运维流程、培训、安全作业、公告通知管理。对于违反相关规范的行为，甲方有权要求乙方按照合同金额的【3‰】支付违约金，违约金从本合同明确的付款中扣除或由乙方进行补缴。

十六、不可抗力

1．不可抗力的内容包括地震、台风、水灾、战争及其他不能预见的不可抗力事故或因国家法律和政府政策调整致使直接影响本合同的履行或者不能按约定的条件履行的情形。

2．签约双方任何一方由于不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，其延长的期限以双方协商一致的结果为准。但合同价格不得调整。

3．受阻一方应在不可抗力事件发生后尽快通知对方，并于事件发生后【14】天内向对方提供有关部门出具的证明。一旦发生不可抗力事件的影响持续【120】天以上，双方应通过友好协商，在合理的时间内达成进一步履行合同的协议。

4．不可抗力事件发生后，相关各方均应采取一切必要的措施减少不可抗力事件所造成的损失。

5．因不可抗力造成的违约，根据不可抗力的影响程度，免除违约方部分或全部应负的违约责任，但法律另有规定的除外。对于本合同的履行，双方协商解决，根据情况决定是否终止本合同。

6．不论发生何种不可抗力事件，其影响仅限于项目受阻部分，其他未受影

响的部分应照常进行。

十七、争端解决

1．双方在执行合同过程中所发生的一切争议，应本着诚实信用原则，通过协商方式解决。如协商不成，可向甲方所在地有管辖权的人民法院起诉。

2．在诉讼期间，除正在进行诉讼的部分外，合同其他部分继续执行。如争议部分严重影响整体合同目的的实现，则应暂停合同执行。

十八、通知和送达

1．本合同要求合同双方发出的通知或其他通讯，应用中文书写，并用专人递送、信函或电子邮件发至对方在本合同封二所列地址，合同一方地址如有改变，应提前【3】天书面通知对方，否则仍以变更前的地址为有效的送达地址，任何一方按照本条款确定的地址进行送达的，视为有效的送达。

2．甲乙双方因履行本合同或与本合同有关的一切通知都应按照本合同封二约定的联系方式，以书面信函形式或双方确认的传真、电子邮件或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达，以回执上注明的收件日期为送达日期，无注明日期的自交邮后第【7】日视为送达。如使用传真、电子邮件或类似的通讯方式，通讯发出之日即视为送达。

3．本合同封二所示的联系信息的适用范围（含电子送达方式）包括但不限于各类告知书、通知书、工作联系单、协议文件、诉讼或仲裁文书，送达主体可以是各方、人民法院、仲裁机构及各行政机关。

十九、合同声明

1．除另有约定外，本合同中的词语和术语的含义与合同条款中的定义相同。

2．双方对所提供的技术资料及价格负有保密的义务，如违反本规定，使对方遭受损失，对方有提出赔偿经济损失的权利。

3．如合同及附件、招标（采购）文件、投标（响应）文件等条款发生冲突，以有利于甲方利益的条款为准；如合同双方对条款意思理解发生争议，以有利于甲方利益的解释为准。

4．乙方在此保证全部按照合同的规定向甲方提供系统、设备和服务，在乙方没有任何违反合同约定的行为的前提下，甲方将按照本合同向乙方支付合同价款。

5．验收之后对系统、设备、服务质量等产生争议，合同双方认为有必要提请有关部门处理的，请在发生争议之日起【2】个工作日内采用书面形式将有关情况报有关部门。

6．本合同一式【陆】份，甲方执【叁】份，乙方执【叁】份，各份均具有同等法律效力。

二十、合同附件

1．项目运维服务管理规范

2．网络及数据安全管理要求

3．分项报价表

4．保密协议

5．廉洁共建合作协议

6．项目成员表

【本页以下无正文】

【本页无正文，为《2023 省工业和信息化厅网络安全维护项目运维服务合同》专属签署页。】

甲方：贵州省工业和信息化厅（盖章）

法定代表人或授权代表（签字）：

签字日期：2024.1.25.

乙方：联通数字科技有限公司贵州省分公司（盖章）

法定代表人或授权代表（签字）：

签字日期：

附件 1：项目运维服务管理规范

项目运维服务管理规范

为确保甲乙双方顺利进行本项目的合作，进一步提高项目的运维服务质量和水平，充分调动乙方积极性、主动性，加强项目管理和考核，特制定本管理规范。

一、最终用户

贵州省工业和信息化厅

二、服务内容

（一）贵州省工业和信息化厅，网络安全维护项目

1．服务方式：远程服务/现场运维

2．详细服务内容：

2023 省工业和信息化厅网络安全维护项目主要采用远程+驻场服务方式运维。主要提供服务包括：

（1）运维内容：漏洞扫描服务、安全基线核查和加固服务、渗透测试服务、风险评估服务、网络分析与优化服务、安全策略管理服务、应急响应服务、应急演练服务、局域网等保二级安全制度建设管理服务、驻场运维服务、备品备件等。

（2）运维指标：提供 5×8 小时运维服务及 7×24 小时电话服务，响应时间不得超过半小时，如需现场处理 4 小时内到达现场；重大事项及活动期间需提供 24 小时保障服务。

（3）服务方式:采用远程+驻场服务方式，驻场 1 人，具备本科学历、计算机专业，满足网络安全服务需求。

（4）服务期限：12 个月（2023 年 4 月 1 日至 2024 年 3 月 31 日）。

（二）服务内容及时间

1．乙方根据甲方要求提供如下服务：

1.1 数据库维保服务

（1）数据库标准服务

1）热线电话支持

提供 7 天×24 小时电话技术支持服务，帮助解决提出的疑难问题。对用户的问题进行技术咨询、指导。

2）专家在线支持

服务期内，用户可以向工程师通过邮件及微信、QQ 等即时通讯与工程师直接沟通，获得技术支持及文档获取。

3）远程接入支持

通过技术支持系统与客户系统进行连接，远程对客户问题进行检查、分析、诊断和解决。工程师仅在得到客户许可的情况下才会访问客户系统，并且会确保访问的安全性，以及保证数据的完整性。

4）完善备份和监控

完善客户提出要求的数据库的备份和监控策略。并且保证保证备份和监控的时效性和有效性。保证数据库无法提供稳定高效服务的情况下及时发现，并通过邮件通知到客户和我们的支撑工程师。保证备份的及时性可可用性。保证在数据丢失或硬件发生的故障下，数据可恢复。

（2）数据库深度健康检查服务

1）检查内容：

检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患。

通过数据库的数据访问（逻辑读、物理读）分析，评估数据库压力状况。

除基本数据库信息检查外，还包括生产环境软硬件环境检查。

主机系统健康检查。

通过工具部署进行主机资源使用状况检查。

数据库系统主机参数检查与调整建议。

存储与备份设备的检查。

数据库系统与主机故障的排查。

检查数据库系统是否需要应用最新的补丁集。

检查数据库空间的使用情况，分析数据量增长趋势。

网络连接状况检查。

数据库特殊对象、大对象的检查，提供特殊或重要表的维护建议。

检查数据库备份的完整性。

协助用户部署合理的数据库性能监控手段，及时分析数据库性能状况，并且及时解决数据库遇到的性能问题。

2）检查方式：现场巡检

检查结果：实施现场巡检后由我们技术人员向用户提供完善的健康检查报告，总结数据库运行状况，分析不足，提出合理化建议。

（3）数据库故障紧急救援服务

1）故障援助范围：

存储设备故障：硬盘损坏、Raid 信息损坏、Raid 组损坏多块硬盘、误删除文件、误格式化硬盘、ASM 磁盘组损坏等。

数据库故障：数据文件坏块、System 表空间损坏、数据文件丢失、归档日志缺失、ASM 故障等。

操作故障：由于误操作等人为原因造成故障致使业务中断的，保留故障现场，由我们专家排查错误，恢复数据库的运行。

2）故障援助说明：

A 级故障（特大故障），即软件系统程序不能启动或启动后不可操作，相关业务系统出现严重问题，业务无法进行，对业务运营造成重大影响。

7*24 小时响应。接到客户方故障申告后，10 分钟内响应，安排二线技术专家远程 20 分钟内介入处理。

B 级故障（重大故障），软件系统程序可以启动，程序出现错误，但关键业务可以运行，严重影响和限制了部分业务运营。

7*24 小时响应。接到客户方故障申告后，10 分钟内响应，安排二线技术专家远程 30 分钟内介入处理。

C 级故障（一般故障），一般性技术故障，程序基本正常，偶尔出现非致命性错误，业务基本不受影响。

7*24 小时响应。接到客户方故障申告后，10 分钟内响应，安排二线技术专家远程在 1 小时内介入处理。

（4）数据恢复服务

服务内容及费用视恢复数据量和恢复难度而定。

三、服务标准

（一）服务响应

乙方应按照甲方管理规范，根据最终用户各系统的重要性和运维事件的紧急

程度，划分运维服务级别，制定相应的服务响应指标，具体情况如下：

服务响应等级及指标表

控制指标	一级	二级	三级	四级
业务重要性	非常重要	重要	较重要	一般
系统年可用率	≥99.95%	≥99.5%	≥98%	≥95%
年无故障运行时间	8756h	8716h	8585h	8322h
服务支持时间	7×24h	7×24h	7×24h	法定工作时间
服务响应时间	≤10min	≤0.5h	≤1h	≤4h
	驻场，即时响应	驻场，即时响应	驻场，即时响应	驻场，工作时间响应
故障恢复时间	一般故障≤1h 重大故障≤2h	一般故障≤2h 重大故障≤8h	一般故障≤12h 重大故障≤36h	一般故障≤24h 重大故障≤72h

若不能按照上述服务响应标准及时处理故障，乙方要组织技术专家对故障进行诊断，并出具解决方案，处理过程及时向甲方和最终用户报告。

（二）服务报告

乙方应针对不同服务响应等级指标出具服务报告，在例行操作、响应支持、优化改善、调研评估服务过程中产生的成果及交付物主要包括巡检报告、运行报告、故障修复报告、分析改进报告、优化改善方案、调研评估分析报告等服务报告，不同类型项目的运维服务报告涵盖的内容如下。

1．应用系统运维

应用系统运维服务报告及主要工作内容包括：

（1）实时或定期巡查业务应用运行状况，包括业务应用运行状态、分析业务应用日志等服务。

（2）定期对业务应用进行例行维护，包括业务应用健康检查，安全审计；数据的校核、清理；业务应用性能分析、优化；登录口令定期修改等服务。

（3）根据需要对业务应用进行响应式维护，包括权限变更、业务流程调整等配置变更；数据的添加、修改、删除及导入、导出；补丁升级等服务。

（4）根据用户单位需求进行软件功能性完善等开发工作。

（5）根据服务级别要求按时修复发生的业务应用故障。

（6）定期进行总结评估，对业务应用运行状况及运行维护工作情况进行分析，提出改进意见。

（7）做好业务应用技术资料的收集、整理；做好运行维护工作过程文档的收集、存档。

（8）乙方应提供日常巡检、例行维护、响应性维护、功能完善、故障处置、分析总结、资料整理等服务，系统运维服务报告响应频次如下：

系统运维服务报告响应频次表

工作内容	一级	二级	三级	四级
服务报告	每月	每月	每季度	每季度

2．机房及硬件设备运维

硬件设备运维服务报告及主要工作内容包括：

（1）定期对网络、服务器、存储、终端等硬件设备进行巡检，查看并记录设备运行状况及告警信息。

（2）实时或定期巡查网络、服务器、存储、终端等硬件设备运行状况。

（3）定期对网络、服务器、存储、终端等硬件设备进行例行维护，根据需要对网络、服务器、存储等硬件设备进行响应式维护。

（4）根据服务级别要求按时修复网络故障。

（5）定期进行总结评估，对网络、服务器、存储、终端等硬件设备运行状况及运行维护工作情况进行分析，提出改进意见。

（6）做好网络、服务器、存储等硬件设备技术资料的收集、整理，定期提交设备清单，定期绘制、更新详细网络拓扑等相关图纸，做好运行维护工作过程文档的收集、存档。

（7）乙方应为网络、服务器、存储、终端等硬件设备提供日常巡检、例行维护、响应性维护、故障处置、分析总结、资料整理等服务，硬件设备运维服务报告响应频次如下：

硬件设备运维服务报告响应频次表

工作内容	一级	二级	三级	四级
服务报告	每月	每月	每季度	每季度

3．网络和基础设施租赁运维

网络、基础设施租赁包括租赁运营商网络专线、机柜机房、短信息服务等基础设施服务。

乙方应为网络、基础设施租赁提供日常巡检、例行维护、响应性维护、故障处置、分析总结、资料整理等服务，网络和基础设施租赁维护服务包括响应频次如下：

网络和基础设施租赁服务报告响应频次表

工作内容	一级	二级	三级	四级
服务报告	每月	每月	每季度	每季度

4．技术服务支持运维

技术服务支撑为各信息系统配置专业知识技能提供的专业服务，主要采用远程服务、现场服务、远程服务+现场服务等服务方式。

乙方配置技术服务支撑人员，为用户单位信息系统提供日常巡检、例行维护、响应性维护、功能完善、故障处置、分析总结、资料整理等支撑服务，技术服务支撑服务报告响应频次如下：

技术服务支撑服务报告响应频次表

工作内容	一级	二级	三级	四级
服务报告	每月	每月	每季度	每季度

5．运维项目服务定级

运维项目服务标准定级如下表所示：

运维项目服务标准等级表

序号	项目名称	服务等级	备注
1	2023 省工业和信息化厅网络安全维护项目	二级	/

乙方应严格执行相关服务标准，在日常运维过程中记录运维过程，形成相应的交付文档，并及时提交甲方，核查是否达到服务标准。并对交付物实行文档过程管理。

四、服务要求

（一）服务人员管理要求

1．乙方应建立运行维护服务相关的人员储备计划和机制，确保有足够的人

员以满足与甲方约定的当前和未来的运维业务需求。

2．乙方应建立运行维护服务相关的培训体系或机制，在制定培训时应能够识别培训需求，并实施对运维人员的培训，确保运维人员具备相应的运维技术能力。

3．乙方应建立运行维护服务相关的绩效考核体系或机制，并能够有效定期对人员进行绩效考核。

4．乙方应提供专业化、梯队化的运维服务团队，明确岗位结构及工作职责：

（1）管理岗人员及职责：

A．在运行维护服务中负责管理运行维护服务；

B．与甲方建立顺畅的沟通渠道，准确地将甲方的需求传递到运维团队；

C．规划、检查运维服务的各个过程，对运维服务的全部内容负责。

（2）技术支持岗人员及职责：

A．在运行维护服务中负责技术支持，包括网络、操作系统、数据库、中间件、应用开发、硬件、集成、信息安全等；

B．对运行维护服务过程中的请求、事件和问题做出响应，保障信息安全并对处理结果负责。

（3）操作岗人员及职责：

A．在运行维护服务中负责日常操作的实施；

B．根据规范和手册，执行运行维护服务各过程，并对其执行结果负责。

5．乙方运维人员应自觉遵守甲方和用户单位各项规章制度，按照各项规章制度办事，服从甲方管理安排。

6．乙方运维人员应严格遵守甲方和用户单位的考勤时间，不得随意迟到、早退、无故旷工，不随意离开工作岗位，随时保持联系畅通。

7．乙方运维人员必须明确工作职责，端正工作态度，对待工作认真负责。

8．乙方运维人员不得利用工作时间从事与运维工作无关的事情，杜绝与运维工作无关的活动。

9．运维人员应妥善保管各类与运维工作相关的文件、资料，防止丢失，严禁外传。

（二）日常例行维护要求

1．乙方在履行本合同过程中，应定期梳理、更新运维对象的资产清单，保证资产的准确性，配合甲方完成资产盘点。

2．乙方应对业务系统的服务器、网络、应用系统、系统软件等进行定期监控和不定期优化，保证业务系统稳定可靠运行。日常例行维护作业内容如下：

日常维护作业表

维护作业分类：服务器		**作业时间：**
类别	**内容**	**作业周期**
服务器性能检查	检查 CPU 占用率、I/O 效率、内存占用、内存换页情况、主要文件系统剩余空间等	1 次/日
服务器进程检查	对操作系统进程状态进行监控检查，对双机系统集群运行状态进行检查。	1 次/日
维护作业分类：网络		**作业时间：**
类别	**内容**	**作业周期**
网络连通性检查	对服务器间的网络连通性进行检查。	1 次/日
维护作业分类：应用		**作业时间：**
类别	**内容**	**作业周期**
应用进程监控	监控应用系统进程的运行状态，是否有告警信息；监控应用进程质量，是否存在无效无用进程。	1 次/日
资源占用情况	查看应用进程对主机资源和数据库资源的占用情况。	1 次/日
日志检查	定时检查运行日志，关注是否有异常信息。	1 次/日
维护作业分类：系统软件		**作业时间：**
类别	**内容**	**作业周期**
系统软件性能检查	A.检测数据库使用 CPU、内存和存储空间占用率，监测进程所占内存大小、监测数据库的表空间利用率、监测数据库 I/O、监测回滚段使用状况、监测数据库锁的数量。 B.检查中间件及第三方管理软件 CPU、内存使用情况，中间件有关的业务处理。	1 次/日
系统软件告警检	检查数据库、中间件及第三方管理软件系统日志是否	1 次/日

查	有告警信息。	

例行维护作业表

维护作业分类：服务器	**作业时间：**	
类别	**内容**	**作业周期**
服务器系统性能数据分析	根据日常维护采集数据汇总形成服务器系统性能数据分析表	1 次/月
编写服务器系统性能分析报告	根据服务器系统性能分析表编制性能分析报告	1 次/月
服务器系统垃圾文件清理	根据日常维护采集数据进行垃圾文件清理	1 次/月
修订服务器系统配置文档	更新服务器系统配置、操作系统软件版本及补丁版本及变更情况相关文档。	1 次/月
服务器安全检查	检查服务器安全参数、检查审计日志，分析安全事件。	1 次/月
服务器账号检查	对操作系统用户账号定期进行复核，保证系统中账号设置与实际工作需求一致，过期账号或离岗员工账号应及时进行清理。	1 次/月
维护作业分类：网络	**作业时间：**	
类别	**内容**	**作业周期**
网络系统性能数据分析	根据日常维护采集数据汇总形成网络系统性能数据分析表。	1 次/月
编写网络系统性能分析报告	根据网络系统性能分析表编制性能分析报告	1 次/月
修订网络系统配置文档	更新网络系统配置、网络数据配置、操作系统软件版本及补丁版本及变更情况相关文档。	1 次/月
网络账号复核	对网络设备用户账号定期进行复核，保证系统中账号设置与实际工作需求一致，过期账号或离岗员工账号应及时进行清理。	1 次/月
维护作业分类：应用	**作业时间：**	
类别	**内容**	**作业周期**
性能指标采集分析	采集应用系统的性能指标，并进行分析，对超出正常阀值的异常情况提交开发商进行程序优化。	1 次/月

优化建议	A.研究现有正常业务处理流程和异常业务处理流程，发现问题，提出优化和改进建议； B.研究并提出方便系统维护、提高维护效率的维护工具要求。	1 次/月
维护作业分类：系统软件	**作业时间：**	
类别	**内容**	**作业周期**
系统软件系统性能数据分析	根据日常维护采集数据汇总形成数据库、中间件及第三方管理软件系统性能数据分析表。	1 次/月
系统软件性能分析	根据数据库、中间件及第三方管理软件系统性能分析表编制性能分析报告。	1 次/月
数据清理	制定数据清理机制、并据此对数据库进行数据清理。对中间件及第三方系统管理软件进行垃圾文件及垃圾数据清理。	1 次/月
修订系统软件系统配置文档	更新数据库、中间件及第三方管理软件系统配置、系统软件版本及补丁版本及变更情况相关文档。	1 次/月
数据库备份	制作数据库备份策略及备份计划，并依据备份计划进行备份、定期检查备份的完成情况。	1 次/月
数据库备份恢复测试	定期组织对数据库备份进行恢复测试，保证备份数据的有效性。	1 次/月
数据库安全检查	定期检查数据库安全参数、审计日志，对安全事件进行分析。	1 次/月
系统软件账号检查	对数据库、第三方管理软件账号定期进行范围和性质复核，保证系统中账号设置与实际工作需求一致，过期账号或离岗员工账号应及时进行清理。	1 次/月
系统软件系统巡检	数据库、中间件及第三方管理软件的健康性检查，并形成检查报告，在检查结束后应对发现的问题落实整改措施并组织实施完成。	1 次/月

3．乙方应对 IDC 机房的物理环境、基础设施、服务器、网络设备、安全设备等进行定期监控和不定期优化，保证 IDC 机房正常运行。维护作业内容如下：

日常维护作业表

维护作业分类：服务器	**作业时间：**	
类别	**内容**	**作业周期**

服务器告警检查	检查服务器系统状态灯是否告警，系统日志是否有告警信息，检查服务器面板显示是否告警，检查服务器附属设备状态灯是否告警	1 次/日
服务器常规检查	检查服务器系统设备之间的连接线路是否接触良好。服务器系统必须保持良好的接地；对服务器的磁带机、光驱、网卡进行检查，保证设备可用。	1 次/日
服务器配置检查	检查服务器系统配置,双机切换配置。	1 次/日
维护作业分类：网络	**作业时间：**	
类别	**内容**	**作业周期**
网络告警检查	检查网络系统状态灯是否告警，系统日志是否有告警信息，检查网络面板显示是否告警，检查网络附属设备状态灯是否告警	1 次/日
网络常规检查	检查网络系统设备之间的连接线路是否接触良好，应及时维护和更换。	1 次/日
网络安全检查	检查网络安全参数、检查网络设备日志，对安全事件进行分析。	1 次/日
网络系统巡检	网络系统的健康性检查，在检查结束后应对发现的问题落实整改措施并组织实施完成。	1 次/日
维护作业分类：基础设施及物理环境	**作业时间：**	
类别	**内容**	**作业周期**
支持性设施（例如电、UPS、通风和空调、消防）常规检查	定期检查和测试支持性设施的功能，降低支持性设施故障或失效带来的风险	1 次/日
机房清扫	对机房进行清扫，保证机房内环境整洁	1 次/日
人员进入使用监控	全程陪同进入机房的人员，实时监控人员的行为，保证人员在机房中操作规范	实时
机房温度、湿度监测	每天 24 小时对机房环境进行监控，包括机房温度、湿度变化等情况，发现问题及时进行处理	实时

五、服务考核

（一）考核办法

1．服务考核采用量化评分的方式进行考核评分，考核总分为 100 分。甲方

依据本办法对乙方进行考核，考核结果作为项目验收、合同付款（扣款）、合同续签的参考依据。

2．乙方在执行该项目所涉及的所有运维或质保服务时，应严格参照“运维管理平台”中具体列明的相关要求，该要求同时作为对应运维及质保服务的验收及考核标准之一。

（二）考核周期

考核周期为合同有效期，按照合同有效期进行年度考核（合同结束后考核）。

（三）考核标准

考核主要包括交付物质量、日常巡检、运维服务等方面，具体要求在“考核细则”处进行约定。

（四）考核流程

1．甲方在服务考核时间节点前【30】天内，根据“考核细则”对项目开展全面的考核评估，形成书面的考核结论和评分，并同步提供给乙方。

2．在书面的考核结论和评分提供给乙方后的【7】天内，甲乙双方就书面的考核结论和评分进行签字盖章确认。

3．甲方根据签字盖章确认后的考核结论和评分，作为项目验收、合同付款（扣款）、合同续签的参考依据。

（五）成绩运用

在年度考核中：

1．考核评分 80 分及以上为考核通过。

2．大于等于 60 分并小于 80 分，扣除合同总金额的【1%】作为违约金；

3．考核评分小于 60 分，扣除合同总金额的【2%】作为违约金。

4．在考核中扣除的违约金，在合同付款时直接从付款金额减扣。

（六）考核细则

考核指标	默认分值	评分标准
交付物质量	10	按照《项目运维服务管理规范》和合同各项运维要求，完成各个阶段文档交付工作，且文档被甲方认可。 1．交付物提交不及时，每次扣 1 分。 2．交付物质量不合格，每次扣 2 分。

考核指标	默认分值	评分标准
		3．每缺失一个阶段的文档交付物，每次扣 5 分。 4．交付物提交不及时，并且质量不合格，且发生两次及以上，每次扣 10 分。
日常巡检	5	每日对系统的主要应用功能进行例行晨检，每周对系统应用程序、操作系统、数据库、中间件、硬件设备等进行巡检，根据安全要求及时更新补丁和修复漏洞，定期开展数据备份。 1、未按上述要求开展相关工作的，每出现一次扣 1 分。 2．因未进行日常检查，或因检查不彻底、发现隐患不及时，最终导致系统出现故障的情况，每出现一次扣 5 分。
运维服务	30	运维服务要符合《项目运维服务管理规范》和合同各项运维要求，提供的运维服务需要获得甲方的认可。 1、未按照《项目运维服务管理规范》和合同各项运维要求开展工作，导致不良影响的，每次扣 2 分；造成严重后果的，每次扣 10 分。造成特别严重后果的，每次扣 20 分。 2．运维服务过程中，受到甲方的投诉电话，每次扣 20 分。 3. 乙方单位在运维服务过程中受到甲方的书面表扬的，每次加 10 分。
应急响应和故障处置	20	要符合《项目运维服务管理规范》和合同各项运维要求，对系统和服务出现的紧急情况及时响应并妥善处理，处理情况及时反馈甲方。 1．出现紧急情况，在 10 分钟内未响应，每次扣 1 分；在 30 分钟内未响应，每次扣 5 分；1 小时内未响应，每次扣 10 分；1 小时以上未响应，每次扣 20 分。 2．因乙方单位原因，造成系统（或关键功能）大范围中断、系统访问缓慢（响应时间在 30 秒以上），大量用户无法正常开展工作的情况，故障时间在 10 分钟以内，每次扣 5 分；30 分钟以内，每次扣 10 分；1 小时以内，每次扣 20 分，每增加 1 小时加扣 10 分。 3．日常故障处理之前，没有征得甲方的同意，私自进行运维操作的，每次扣 20 分。 4．针对与乙方服务范围内无关的突发情况，乙方及时配合甲方，起到决定性的作用并妥善处理，使甲方的损失降到最小，每次加 10 分。
重大活动及节假日	20	重大活动及节假日保障工作是指在重大活动或者特殊时期进行运维和安全保障，无任何安全事件发生。

考核指标	默认分值	评分标准
保障工作		1．因保障力度不够，没有造成安全事件发生，但是产生不良影响的，每次扣 10 分； 2．因保障力度不够，造成安全事件发生的，每次扣 20 分。
沟通、协调	5	与本单位运维团队紧密衔接工作，并能与甲方、其他项目运维单位保持良好沟通和协作。 1．不能有序、有效开展上述协作的，影响项目进展情况的，每次扣 1 分。 2．沟通协调过程中态度恶劣，没有责任心的，每次扣 2 分。 3．沟通协调过程中出现谩骂、不尊重人的，每次扣 5 分。
工作态度	5	根据甲方的要求完成项目范围内交办的有关工作。 1．能够完成交办的工作，但完成的及时性、准确性方面存在不足，每次扣 1 分。 2．针对甲方交办工作，30 分钟内没有积极响应的，每次扣 2 分。 3．不接受、不配合交办的工作，每次扣 5 分。
工作评价	5	对项目范围内的各项工作开展情况随机进行 2~3 次的评价，由甲方评价。 1．评价为一般，每次扣 1 分。 2．评价为不满意，每次扣 2 分。 3．评价为极度不满意，每次扣 5 分。

附件 2：网络及数据安全管理要求

网络及数据安全管理要求

一、日常运维工作管理要求

1．乙方在信息系统日常操作及维护管理，包括主机操作系统、应用系统、网络设备和安全设备，都应指派专门的系统管理人员开展。乙方应制定《信息系统日常操作及维护管理责任表》，责任到人，确保信息系统正常稳定运行。

2．乙方应按照合同要求，负责开展系统、网络、设备巡检服务，根据相关系统运维手册规范操作，巡检内容严格按照服务合同的约定。

3．乙方工作人员对信息系统的所有操作都必须进行记录，日常维护操作应在工作日报中进行说明。对信息系统进行较大操作或修改前，必须提交修改方案及申请，对在日常巡检中发现的问题，应按照事件管理中的相关要求，及时进行处理。

4．为了保证操作系统日志处于运行状态，应定期对日志进行审计分析，至少每月审计一次，重点对登录的用户、登录时间、所做的配置和操作做检查，在发现有异常的现象时及时向甲方报告。

二、网络及数据安全管理要求

1．乙方应严格按照国家网络安全法律法规的要求，构建网络安全防范机制，制定网络安全管理制度和技术要求，杜绝网络安全事件的发生。

2．按照“谁服务、谁负责”的原则，乙方应提供网络安全的保障机制，建立网络安全的监测机制和风险管理措施，确保网络及数据安全。

3．乙方应为项目驻场运维人员提供专用计算机设备及安装甲方要求的终端管控软件，并要求所有人员签署保密协议（保密承诺书）、背景审查（无犯罪证明）、数据安全责任书。

4．乙方应配合甲方组织的网络及数据安全检查工作，按照甲方要求提供材料并配合检查工作。

5．安全事件的等级划分为特别重大事件、重大事件、严重事件和一般事件。

（1）特别重大事件

因网络安全事件造成网络大面积中断、业务大面积瘫痪或相关业务数据泄

露，对甲方或最终用户造成巨大经济损失或产生严重不良社会影响的；因承载网络中断，造成三分之二以上用户单位不能正常使用业务系统，持续时间达【12】小时以上的。

（2）重大事件

因网络与信息安全突发事件造成网络较大面积中断、业务系统较大面积瘫痪、相关业务数据丢失或遭到篡改，造成重大经济损失或产生较严重不良社会影响。

（3）严重事件

因网络与信息安全突发事件造成网络中断、业务系统瘫痪、相关业务系统数据毁坏，有关信息发布和传播系统发生政治敏感信息事件，造成较大经济损失或产生一定程度不良政治影响和社会影响的。

（4）一般事件

因网络与信息安全突发事件造成网络中断、业务系统瘫痪、部分业务系统数据毁坏，造成一定的经济损失和社会影响的。

6．发生安全事件时，应遵照最终用户单位、甲方应急预案执行，并严格按照应急预案所规定的步骤快速实施应急处置，及时汇报上级领导，掌握实时处理情况。

7．在处理过程中，如需其他部门现场增援处理的，应及时向上级领导部门汇报，协调沟通技术支撑赶赴现场处理。

8．安全事件发生后，依据安全事件造成的影响开展工作考核，采用积分制，考核标准如下：

（1）发生一次一般安全事件的，每发生一次，记 1 分；

（2）发生一次严重安全事件的，每发生一次，记 2 分；

（3）发生一次重大安全事件的，每发生一次，记 3 分；

（4）发生一次特别重大安全事件的，每发生一次，记 5 分；

9．网络安全、数据安全的主管单位包含市级主管单位、省级主管单位及国家级主管单位，如网安、网信、省大数据局等。如被以上主管单位通报的，按照以下标准考核：

（1）被市级主管单位通报的，记 1 分；

（2）被省级主管单位通报的，记 3 分；

（3）被国家主管单位通报的，记 5 分。

10．不配合甲方组织开展网络及数据安全检查工作的，一次记 3 分。

三、安全服务考核

1．甲方对乙方的安全管理开展季度考核。考核结果直接影响服务评价和合同续签。

2．考核结合综合评价和考核积分两个方面，将考核等级分为优秀、一般、达标和不达标四档。考核内容按照与乙方签订的运维服务合同内容具体制定，解释权归属甲方。

考核评分表和等级判定表如下：

等级	评价条件	备注
优秀	同时满足下列条件： （1）很好地履行合同，现场服务力量充足，高度重视安全管理工作，完全满足业务部门开发、运维需求，得到业务部门的一致好评。 （2）运维期内未发生任何安全事件。	
一般	同时满足下列条件： （1）较好地履行合同，现场服务力量能满足服务需求，重视安全管理工作，事件响应及时，能满足业务部门开发、运维需求，得到业务部门认可。 （2）1≤安全事件积分＜4。 （3）运维期内未发生过重大事件或特别重大事件。	
达标	同时满足下列条件： （1）基本能够履行合同，现场服务力量基本满足需求，缺乏有效安全管理手段，对事件响应及时，勉强能满足业务部门服务需求，业务部门对服务评价一般。 （2）4≤安全事件积分＜8。 （3）运维期内仅发生过 1 次重大事件。 （4）运维期内未发生过特别重大事件。	
不达标	满足下列条件之一： （1）不能很好地履行合同，现场服务力量不足，完全不重	列为不达标供应商并列入供

	视安全管理工作，对事件多次响应不及时，不能满足业务部门服务需求，业务部门对付服务评价不合格或很差。 （2）8≤安全事件积分。 （3）运维期内发生过 2 次及以上重大事件或 1 次特别重大事件。	应商灰名单

3．甲方将按照安全管理考核结果对乙方进行处罚。

（1）【优秀】不进行处罚；

（2）【一般】扣除合同金额的【5%】作为违约金；

（3）【达标】扣除合同金额的【10%】作为违约金；

（4）【不达标】扣除合同金额的【15%】作为违约金。

（5）考核中扣除的违约金，在合同付款时直接从付款金额扣减。

附件 3：分项报价表

分项报价表

序号	服务内容	详细规格说明	数量	单位	单价（元）	小计（元）	税率
1	漏洞扫描服务	每月对工信厅局域网资产进行全面的漏洞扫描。对扫描的结果进行人工分析，排除扫描系统误报，出具漏洞分析报告；每月按需对高危风险持续复查、指定漏洞定向检测、持续对 0Day 漏洞进行检测/监控。资产范围：10 个服务器 IP、30 个网络设备、250 终端。（说明：态势感知是流量监测，分析流量日志，漏洞扫描是主动给业务系统扫描漏洞。（被动与主动））。 服务周期：12 次/年，16 个系统。	1	项	￥65,000.00	￥65,000.00	6%
2	安全基线核查和加固服务	每半年针对已建立安全基线的 IT 基础设施（包括操作系统等）开展安全基线配置核查，若存在极限配置发生变动，结合实际情况立即展开修复整改，完成后出具 IT 基础设施安全基线配置核查报告。资产范围：10 个服务器 IP、30 个网络设备、250 终端。 服务周期：1 次/年，16 个系统。	1	项	￥40,000.00	￥40,000.00	6%
3	渗透测试服务	高级服务工程师在获得授权的情况下，以主流渗透工具结合自研的工具模拟黑客攻击为主要手段，发现常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，并针对每一安全漏洞提供相应的解决方法。并结合客户修复情况，协助客户针对修复后的漏洞进行复测验证。资产范围：16 个业务系统。 服务周期：16 个系统，1 次。	1	项	￥90,000.00	￥90,000.00	6%
4	风险评估服务	具体工作内容包括评估用户信息系统安全现状，对信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性和对资产造成的影响进行评估，最终提供全面性的风险评估报告。风险评估以技术手段（漏扫、基线等）为基础，结合资产信息进行威胁关联分析，同时访谈业务人员了解安全现状，最终汇总数据分析并整合成风险评估报告。 服务周期：1 次/12 个月,16 个系统	1	项	￥25,000.00	￥25,000.00	6%

5	网络分析与优化服务	每半年按照国家相关安全标准和架构安全性对现有网络架构和安全域其进行分析对比，若存在安全隐患则结合现有业务情况整改，完成后出具网络结构和安全域分析报告或架构整改报告。	2	次	￥12,000.00	￥24,000.00	6%
6	安全策略管理服务	根据业务属性、业务风险与行业安全策略最佳实践相结合制定出最符合业务情况的安全策略，同时具备策略有效性检测机制。新增资产、业务变更时策略随业务变化而同步更新，并提供策略有效性调优服务。对所有网络安全和网络设备合规性检查，并进行整改。 服务周期：1 次/月，12 个月	12	次	￥3,500.00	￥42,000.00	6%
7	应急响应服务	1.勒索病毒事件分析：专家分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等； 2.挖矿病毒事件分析：专家分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等； 3.蠕虫病毒事件：专家确认文件是否被感染，定位失陷的代码并进行修复； 4.根据安全事件发生的根因、影响范围，针对性给出安全加固方案； 5.通过现象深入分析安全事件的成因，发现用户网络中存在的薄弱点，通过技术手段和方法溯源攻击路径； 6.根据安全事件发生的根因、影响范围，针对性给出安全加固方案； 7.提供安全应急响应服务并组织各系统承建商配合开展应急处置，在安全事件发生后保证 2 小时内到达现场开展处置工作，供应商在事后需对安全应急过程进行分析总结。	1	项	￥28,000.00	￥28,000.00	6%
8	应急演练服务	每年组织工信厅各部门针对工信厅局域网开展一次应急演练，模拟安全事件发生后的应急处置流程和工作方式，为真实应急做准备。完成后出具标准的应急演练报告。	1	次	￥32,000.00	￥32,000.00	6%
9	局域网等保二级安全制度建设管理服务	依据国家/国际信息安全标准、信息安全策略及行业发展动态，在对用户信息安全现状进行风险评估、差距分析的基础上，从安全技术、安全管理、安全运营三个角度帮助客户构建短期、中期与长期的信息安全规划，将信息安全的单点风险控制转变为全面的安全规划，进而推动有效的信息安全建设并建立完整的信息安全保障体系。协助用户完善安全管理制度的优化。（说明：管理制度+安全规划）	2	次	￥10,000.00	￥20,000.00	6%

10	驻场运维服务	采用安全专业的安全人员，通过加强对现场的安全的运维，为贵州省工信厅提供日常驻场服务运维、重大节假日保障服务，确保工信厅的网络安全。 驻场人员一：安全运维员 1.参与安全运维体系建立和实施，设计并推进安全运维自动化； 2.保障部门安全运维安全，处理安全运维事故,优化各项维护工作流程，不断降低系统风险； 3.参与基础设施项目交付包括新的或改进的核心基础设施服务、网络、主机、安全等参与新 IT 基础设施的可行性研究。协助厅级软件的选择和 IT 咨询服务。	12	月/人	￥11,000.00	￥132,000.00	6%
11	备品备件	为现有局域网等保服务体系提供保障,UPS 系统作为工信厅局域网等保二级建设需求评审项之一，因此需对 UPS 系统进行提升服务。提供备品备件服务，包含 UPS 备用电池服务及局域网接入交换机备用服务，当 UPS 电源间设备发生故障时，提供规格 12V、100AH 电池进行更换及光模块、千兆交换机 2 台故障时提供服务等。	1	项	￥27,000.00	￥27,000.00	6%
合计						￥525,000.00	

附件 4：保密协议

保密协议

甲方：贵州省工业和信息化厅

乙方：联通数字科技有限公司贵州省分公司

为确保甲乙双方顺利进行本项目的合作，确保本项目建设中涉及的相关信息的保密安全，经协商一致，针对合作过程中涉及到的相关信息，甲乙双方达成如下协议并承诺共同遵守。

一、保密信息的范围

本保密协议所指“信息”包括任何以口头、书面、图表或电子形式存在的以下内容：

1. 任何涉及甲方方过去、现在或将来的人员结构、规章制度、质量体系、工作流程、处理手段、财务信息以及甲方方拥有或使用的系统、平台、终端、存储设备所载信息等；

2. 任何甲乙双方在项目实施中涉及的技术措施、技术方案、软件应用与开发，以及甲方和最终用户方硬件设备的品种、质量、数量、品牌等；

3. 任何甲乙双方在项目实施中涉及的技术秘密或专有知识、文件、报告、数据、软件、流程图、数据库、发明、知识等，无论上述信息是否享有知识产权；

4. 任何甲方方其它的以有形方式或无形方式存在的且不被社会公众知悉的信息。

这些“信息”无论乙方何时接受或接触到，均属保密信息。

二、甲乙双方的保密义务

1. 甲方对乙方提供的技术信息和资料负有保密责任，未经乙方同意不得提供给与本项目无关的任何第三方。

2. 对不再需要保密或者已经公开的技术信息和技术资料，甲方应及时通知乙方。

3. 乙方对于从甲方方处收到的信息，在未经甲方事先书面许可的情况下，不得以任何方式提供给项目之外的第三方及双方的无关人员。

4．乙方对于从甲方方处得到的信息，应当通过建立内部保密制度、培训工作人员保密意识等方式和措施，确保信息的安全。

5．乙方承诺，所收到的甲方方信息只能用于本项目而不得用于任何其他目的。

6．乙方承诺，所收到的甲方方信息在本方此项目工作组中能得到谨慎的使用，只能用于本方参与此项目的相关人员，并且保证该相关人员在知晓信息之前已经充分了解了本协议的内容。

7．乙方承诺，对于所收到的甲方方信息，未经甲方事先书面许可，不得以任何形式复制和传播。

8．除甲方事先书面同意，否则乙方不得向第三方以任何形式透露双方的任何会谈、会议、协商或共同工作的内容。

9．除双方另有约定外，负有本协议约定的保密义务的主体包括：乙方参与或曾经参与本项目的人员、在工作中有意或无意以及可能获悉本协议约定的保密信息的其它人员（包括但不限于乙方的工作人员）。

10．乙方出于完成本项目目的，从甲方处取得的书面或电子信息，应当在项目完成后即时完整地归还甲方。

11．乙方利用自有设备或甲方设备在软件开发调试及设备配置过程中，杜绝发生“一机两用”等违反网络信息安全规定的行为。

12．除非双方书面同意，本协议所规定的保密期限为永久。

13．甲方提供信息的行为不得被视为是以任何方式授予技术许可，或是转让著作权、商标权、专利权或技术秘密的行为。取得甲方信息，并不表明取得了信息的任何知识产权；甲方所提供的任何信息的知识产权和财产权利，全部归甲方所有。

14．如乙方工作人员因完成本项目需要进入甲方或最终用户方工作场所，应当严格遵守甲方方的相关规章制度，不得进入甲方或最终用户方未授权进入的办公区域，不得在与本项目工作无关的区域活动。

三、其他约定

鉴于甲乙双方形成的合作关系，本协议约定的保密义务作为乙方向甲方履行

生产、供货义务的附随义务，甲方不再另行支付乙方保密费用，乙方不得以任何理由及任何方式以本协议为依据向甲方主张权利。

四、违约责任

若一方违反上述任何条款，应当承担本项目合同额【2%】的违约金，如给对方及最终用户方造成损失，违约方还应承担相应的赔偿责任及其它所有法律责任。

【以下无正文，为《保密协议》签署信息。】

甲方：贵州省工业和信息化厅（盖章）　　乙方：联通数字科技有限公司贵州省分公司（盖章）

甲方代表签字：　　乙方代表签字：

签字日期：　　签字日期：

附件 5：廉洁共建合作协议

廉洁共建合作协议

甲方：贵州省工业和信息化厅

乙方：联通数字科技有限公司贵州省分公司

为维护甲乙双方的合法权益，健全和完善监督制约机制，预防职务犯罪行为的发生，保证双方企业依法经营、业务工作人员廉洁从业，根据国家有关法律法规的规定，经双方自愿、平等协商，签订如下廉洁共建合作协议。

1．双方应在遵守国家政策、法规的前提下开展业务交往活动，不得违法经营。充分尊重并配合执行对方有关廉政建设的各项制度及规定。

2．在业务交往活动中，应贯彻平等、互利、公平、协商一致的原则自觉履行经济合同。

3．双方工作人员要廉洁勤政、秉公办事，提高服务质量，讲究工作效率，不扯皮推诿，不刁难对方。

4．双方发生经济往来，必须通过银行结算。业务往来中有关优惠、让利应写入合同，放在明处，不得以任何理由或方式截留。

5．双方工作人员不得擅自发生何形式的借款、租赁及财产买卖关系。

6．双方工作人员不得以任何理由、方式向对方索要或赠送现金、有价证券、支付凭证和高档贵重礼品，以及各种名义的回扣、好处费、感谢费等。不得到对方报销应由本方个人或集体支付的各种费用。

7．双方工作人员不得利用婚丧、乔迁、升学等名义，向对方单位或个人收取或赠送钱财。

8．双方工作人员不得利用职权，卡扣应付款项；不得利用职权以威胁恐吓、不配合等方式干扰合作方的正常工作；不得利用职权以隐瞒包庇、不作为等方式纵容合作方违规操作；不得与第三方恶意串通，以包含但不限于串标、围标、泄露标底、虚报价格、制定虚假方案、虚增工程量、虚办签证、供应伪劣残次材料、设备等方式，损害合作方的合法利益。

9．双方工作人员不得以职权和职务影响或工作便利违规为本方或对方亲朋好友牟利。

10．双方在业务交往中需要招待的，要本着必要、适度、从俭的原则，不得铺张浪费，不得组织、参加不健康的活动和高消费娱乐活动。

11．双方工作人员不得向对方或第三方泄露经济秘密。

12.双方有义务配合对方反馈本协议的执行情况并及时向对方通报本方的廉洁规定，在交流业务的同时要交流廉洁建设的经验，互相监督，共同提高。

13．双方应自觉履行本协议的各项规定。甲方工作人员违反上述有关规定，乙方可向甲方负责人通报，也可以向甲方投诉、举报，甲方将及时向乙方通报查处情况。乙方违反上述有关规定，甲方应向乙方负责人通报，并视情节轻重，按照警告、取消投标资格、取消合格供应商资格及列入黑名单的方式减少或停止与乙方的业务往来，后果由乙方负责。

【以下无正文，为《廉洁共建合作协议》签署信息。】

甲方：贵州省工业和信息化厅（盖章）	乙方：联通数字科技有限公司贵州省分公司（盖章）
甲方代表签字：	乙方代表签字：
举报电话：	举报电话：15685191001
举报邮箱：	举报邮箱：gzs-gyjcs@chinaunicom.cn
签字日期：	签字日期：

附件 6：项目成员表

项目成员表

序号	姓名	项目角色	职责	联系方式
1	徐丽	客户经理	负责与客户整体项目沟通	18685192087
2	苏雄	项目售前经理	负责方案整体规划	18685190906
3	叶松尧	项目管理经理	负责项目实施过程的整体规划	18685190805
4	杨超	网络安全服务人员	负责每日现场网络安全服务及驻场工作	15086314812
5	刘军	项目施工布线调试人员	负责现场网络设备、安全设备调试服务	15692718889