（服务类）

信息系统建设服务合同

项目名称：北京友谊医院顺义院区应用系统与研究所信息化建设项目（医院部分）招标

甲方：首都医科大学附属北京友谊医院

乙方：联通数字科技有限公司

甲方：首都医科大学附属北京友谊医院

地址：北京市西城区永安路 95 号

联系人：刘志军

联系电话：63139390

乙方：联通数字科技有限公司

地址：北京市西城区西单北大街甲 133 号

联系人：郭立冬

联系电话：18601105363

甲方就北京友谊医院顺义院区应用系统与研究所信息化建设项目（医院部分）招标中所需 5G 边缘云管理平台经中技国际招标有限公司以 0701-254106140767/01 号招标文件在国内北京市招标。经评标委员会评定乙方为中标人。甲乙双方同意按照下面的条款和条件，签署本合同。

第一条 服务信息

1、乙方向甲方提供信息系统建设服务的名称为：北京友谊医院顺义院区应用系统与研究所信息化建设项目（医院部分）招标-5G 边缘云管理平台（以下简称“本项目”）。

2、本项目的价款为人民币 1298860 元（大写：人民币壹佰贰拾玖万捌仟捌佰陆拾元整）。合同价款包括但不限于信息系统开发费用、税金、包装、运输、保险、安装调试、培训费、根据法律法规应由乙方承担的税款等本合同项下甲方需向乙方支付的全部费用，除此之外，甲方无需因本合同向乙方支付任何费用。

3、本项目的服务内容详见附件一《信息系统功能需求清单》、附件二《售后服务方案》、附件三《运维服务方案》、附件四《中标通知书》，为本合同不可分割的一部分，与本合同具有同等法律效力。

第二条 乙方主体资格

1、乙方应向甲方提供签订本合同所需的全部资质文件的复印件，在复印件上注明与原件一致并加盖公章。

2、本合同项下，乙方应向甲方提供的乙方的资质文件为：

☑营业执照；

☐软件产品登记表；

☐软件著作权登记证书；

☐专利证书；

☐系统集成企业资质登记证明；

☐营销人员授权书；

☑售后服务承诺书；

☐产品代理授权书；

☐其他：_____/_____。

第三条 付款方式

1、甲方根据北京市财政支付流程向乙方支付合同总价款，合计为人民币1298860元整（大写：人民币壹佰贰拾玖万捌仟捌佰陆拾元整）。

根据北京市财政资金拨付进度，第一期款项不低于合同总价款的60%，此后，甲方根据北京市财政资金到账情况，向乙方支付合同款项。

甲方收到货物并验收合格前，甲方有权不向乙方支付全额款项。

2、甲方每次付款前，乙方应向甲方提供符合甲方要求的发票，甲方确认发票内容及金额无误后，向乙方支付款项。乙方未提供发票，或者提供发票的内容或金额有误的，甲方有权拒绝支付相应款项且无需承担任何违约责任。

3、乙方账户信息如下：

账户名称：联通数字科技有限公司

开户行：中国工商银行股份有限公司北京灵境支行

银行账号：0200013319200042469

4、甲方开票信息如下：

账户名称：首都医科大学附属北京友谊医院

开户行名称：工商银行珠市口支行营业室

开户行账号：0200003109089210458

纳税人识别号：121100004006886096

5、本合同项下支付及结算（☑适用/☐不适用）财政资金支付程序。如本合同项下的支付及结算适用财政资金支付程序的，则以财政资金的支付及结算程序为准，与之相抵触的约定无效。

第四条 甲乙双方的权利及义务

1、甲方的权利及义务如下：

（1）甲方指定专人负责在本合同执行过程中的组织和协调工作。

（2）甲方按需组织协调解决问题，跟踪工作进度。

（3）甲方为乙方现场安装调试和正式部署提供必要的软件、硬件、网络、基础数据等条件，以满足软件安装调试的需要。

（4）为使本项目完成后能更好地进行今后的维护工作，甲方安排一名以上维护人员全程跟踪学习、参与安装调试。

（5）甲方有权知晓各种技术和方案的细节，并提出改进意见。

（6）在任何时候，甲方对乙方负责本项目的专业人员的主要工作表现不满意，可立即书面告知乙方，并可要求乙方更换人员。乙方应采取合理措施，在收到甲方的书面告知后 10 个工作日内予以解决。

（7）乙方（☐需要/☑不需要）向甲方提供源代码。乙方如须要向甲方提供源代码的，甲方应保证源代码的使用仅限于内部进行系统维护使用，未经乙方许可，甲方不得将源代码及修改后的源代码提供给任何第三方。

（8）乙方提供的软件（☐需要/☑不需要）与甲方院内其他系统进行接口。如须要与甲方院内其他系统进行接口的，甲方应负责参与协调接口协议和参与拟定数据标准。

（9）甲方负责及时签收乙方交付的软件及相关产品，按本合同约定进行验收，并按照本合同规定的付款方式及时付款。

（10）其他：无

2、乙方的权利及义务如下：

（1）乙方指定 郭立冬 为乙方的联系人，协调履行本合同的权利和履行义务。乙方联系人的联系电话为 18601105363 。

（2）以下条件符合后，乙方应在 2 个月内完成安装调试、测试、人员培训等系统上线工作，待甲方验收合格后交付甲方正式使用：

☑本合同签订生效后

☐乙方收到甲方根据支付的第一笔合同款项后____/_____内

☐其他：_____/_____

（3）乙方向甲方派遣适合本合同要求的技术人员队伍，并指派专人负责该工作，确保按双方约定的要求保质、保量地完成本项目的开发安装调试工作。

（4）乙方交付的技术服务工作成果应满足网络安全等级保护 3 级基本要求，并服务过程中或在维保期内需无偿向甲方提供对安全漏洞的修复服务。

（5）乙方（☐需要/☑不需要）提供本项目中所含的客户端正版操作系统。

（6）乙方应按照以下约定，及时、主动地向甲方提交书面工作报告，告知工作进展及所须要解决的问题：

☐每日

☑每周

☐其他：_____/_____

（7）乙方应指导甲方相关人员进行基础数据的准备、整理工作。

（8）在整个安装调试过程中，乙方应对甲方相关人员进行软件功能、作用、和使用操作等培训。

（9）乙方应向甲方提供甲方要求的、不涉及乙方保密信息的所有文档及技术资料。

（10）如因乙方原因无法为甲方提供持续的售后服务和产品升级，乙方（☑需要/☐不需要）无偿向甲方提供以下资料，以保证甲方系统的正常稳定运行：

☐源代码；

☑运维手册；

☐数据结构；

☐其他：_____/_____

（11）乙方应根据本合同的相关条款及甲方的要求，对系统提供质保和维修。乙方应保障系统不发生重大故障，否则甲方有权追究乙方相关责任。

（12）未经甲方事先书面同意，乙方不得将本项目涉及的软硬件系统、数据

库、数据、影像等内容进行任何加密设置，不得对甲方应用本项目相关的系统和数据设置任何限制。如乙方认为必须进行加密的，必须事先取得甲方的书面同意，并向甲方提供解密算法。

（13）其他：无

第五条 售后服务条款及质保服务

1、本项目自验收之日起 3 年内为质保期，乙方应提供免费维护服务。

2、质保期内，乙方应向甲方提供如下质保服务：

（1）乙方提供（☑7*24 小时/☐5*8 小时/☐其他：/）技术支持，并不限支持次数。乙方应根据以下的故障等级提供相应的处理：

故障等级	故障等级定义	处理时间及方式
一级故障	系统瘫痪、严重影响系统使用、严重影响其他关键业务正常使用，如：系统无法访问、数据库无法连接等	立即响应，（☑1 小时内/☐/小时内）电话/网络远程支持，并通过最快交通方式到达故障现场，到达现场后 4 小时内解决故障（因特殊原因无法在 4 小时内解决故障的，经甲方同意后可适当延长）。
二级故障	影响系统使用、影响其他关键业务正常使用，如：系统能正常访问，但部分功能模块无法使用。	立即响应，（☑2 小时内/☐/小时内）电话/网络远程支持，12 小时内到达故障现场。到达现场后 4 小时内解决故障（因特殊原因无法在 4 小时内解决故障的，经甲方同意后可适当延长）。
三级故障	轻微影响使用，远程支持后可解决；不影响其他关键业务使用，如：系统自身的 BUG，甲方对系统使用的疑问，对系统新功能的咨询等	（☑30 分钟内/☐/小时内）响应，（☑2 小时内/☐/小时内）内电话/网络远程支持并解决故障（因特殊原因无法在 2 小时内解决故障的，经甲方同意后可适当延长）。

（2）乙方（☑需要/☐不需要）免费为甲方技术人员进行系统管理、操作培训，培训次数不得少于 1 次，具体次数由甲方指定。

（3）乙方提供专门技术服务人员进行项目后期跟踪，提供每年不少于 1 次的（☐现场/☑非现场）服务，及时检查并处理问题。

3、免费维护期内，乙方（☐需要/☑不需要）提供常驻技术支持服务。如乙方须要提供常驻技术支持服务的，乙方应指派 / 名技术工程师常驻甲方。派遣的工程师均应具备相关技术资格认证的工程师，保证提供专业的、正确的和高效的技术服务和技术培训。

4、质保期满后，乙方（☑需要/☐不需要）提供常年维保服务。如乙方须要提供常年维保服务的，甲乙双方应另行签订维保服务协议，每年维护费用为：

☐合同(☐总价款/☐软件部分/☐硬件部分)的 _/__%，即，即人民币 / 元（大写：人民币 /）

☐人民币 / 元（大写：人民币 /）

☑其他：双方另行协商确定

5、乙方（☐需要/☑不需要）向甲方提供本合同中所有系统模块的维护、功能和代码的优化。

第六条 系统验收

1、本项目满足附件一《信息系统功能需求清单》，系统上线稳定运行 1 个月，且甲方相关使用部门签字确认后，由乙方提出书面验收申请。甲方收到乙方的验收申请后，对系统的整个情况进行评估验收。乙方应确保系统的全部有关技术文件、资料、及安装、测试、验收报告等文档完整交付。验收合格后，甲方签署验收报告。验收不合格甲方需书面告知乙方不合格原因，乙方负责按照验收标准整改并再次提出验收申请，直到验收合格。

2、验收时，乙方需向甲方提交包括但不限于以下甲方要求的资料和文件。

☐《总体设计报告》;

☐《需求分析说明书》;

☐《详细设计说明书》;

☐《数据字典》;

☐《操作使用说明书》;

☑《系统运行维护手册》;

□其他：/

3、甲方不得以本合同范围外的软件功能及硬件设备等问题而拒绝或延误项目验收。

第七条 知识产权

1、乙方保证甲方及其用户在使用本合同项下产品、服务及其任何部分时，不会受到任何第三方关于侵犯专利权、商标权、工业设计权或知识产权的质疑。任何第三方如果提出侵权质疑，乙方须与第三方交涉并承担可能发生的一切法律责任和费用。

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

3、在本合同有效期内，乙方利用甲方提供的知识类资料所完成的知识类成果，归甲方所有。

4、由各方各自独立开发的专利以及其他知识产权归属各自所有。

第八条 保密

保密信息是指甲乙双方各自专有的、或提供给对方的并明确标有“保密”字样的信息，包括但不限于本合同及其签订、许可软件、数据等。甲乙双方承认保密信息构成有价值的商业秘密。甲乙双方同意严格按照本合同的规定使用对方的保密信息，未经对方的事先书面许可，不得向第三方，或允许向第三方直接或间接地透露保密信息。本合同的保密义务为永久。无论本合同变更、解除或终止，本条款保持有效。

第九条 违约责任

1、乙方应按本合同约定完成本项目的服务工作，乙方每延迟一日，需支付合同总价款 1%的违约金。延迟交付达 15 日的，甲方有权单方解除本合同，要求乙方返还甲方已支付的合同价款，并承担相当于合同总价款 20%违约金。若因归责于甲方原因导致延迟，或乙方因特殊原因导致延迟且事前取得甲方书面同意的，

乙方不承担违约责任。

2、因乙方未按甲方的网络安全要求执行或实施服务，而造成甲方不良网络安全事件、经济损失、恶劣社会影响，每发生一次，乙方应向甲方支付与损失等价的赔偿金，赔偿金额按每起事故不低于合同总款的5%计算。

3、乙方应确保所提供成果和技术服务的稳健性，因乙方在提供技术服务过程中的过失、疏忽或技术服务工作成果的缺陷，引发的信息系统故障或业务数据损失，而造成甲方经济损失、不良社会影响的，每发生一次，乙方应向甲方支付与损失等价的赔偿金，赔偿金额按每起事故不低于合同总款的5%计算，同时乙方须按甲方要求积极负责排查故障原因，彻底解决问题。

4、乙方未能在本合同规定时间内到达现场或解决故障的，每延迟4小时，需支付合同总价款1%的违约金。但因特殊情况，甲方同意适当延长故障解决时间的除外。

5、乙方在接到甲方的维修要求后24小时内未能解决故障的，甲方有权指定第三方提供服务，由此造成的额外费用及给甲方造成的损失均由乙方承担。

6、乙方出现违约3次以上（含3次）的，或者延迟时间累积24小时（含24小时）时，甲方有权单方解除本合同，并要求乙方支付相当于本合同总价款20%的违约金。

7、乙方违反保密义务，造成甲方损失的，应支付甲方与泄密内容和不良影响等价的赔偿金，赔偿金额按每起事故不低于合同总款的60%计算。

8、违约金不足以弥补甲方因此遭受的损失的，乙方还需就不足部分承担赔偿责任。

9、甲方有权从剩余应向乙方支付的款项中优先扣减乙方应向甲方支付的款项（包括但不限于违约金、赔偿金等）。

10、乙方未按本合同约定提供服务的，甲方有权要求乙方延长免费维护期。延长的免费维护期限由甲方决定。如乙方对甲方提出的维护期限有异议的，应提出书面异议并说明理由。乙方提出书面异议的，甲乙双方通过协商决定延长的免费维护期限的时长，但该免费维护期限不得低于乙方未按照本合同约定提供服务的合计时长。

第十条：信息集成

乙方应确保所提供成果和技术服务满足甲方的信息集成要求：

1、业务字典需通过甲方信息集成平台与主数据系统对接；

2、业务数据要求需按照甲方标准接口定义通过信息集成平台进行对接；

3、信息系统中业务数据需根据甲方需求，支持但不限于数据库同步、视图、接口等集成方式开放；

4、支持 HL7 V3、HL7 FHIR 等国家或行业标准，以及甲方自定义标准接口对接；

5、支持各类传输访问协议，包括但不限于 HTTP/HTTPS、TCP/IP、SFTP、SOAP/HTTP；

6、支持满足安全要求的数据存储及传输的加密/解密；

7、支持根据甲方需要的数据或业务功能提供符合需求的 API 服务；

8、需按照甲方需求与其它信息系统进行表示、数据、控制、业务流程等方式的集成。

第十一条 国产化适配要求

乙方应按甲方要求配合进行国产化适配和替代，以确保所提供的信息系统能够在国产操作系统、国产数据库、国产中间件等国产基础软件环境中运行和使用，所有功能保持一致，性能确保稳定，包括服务端。

第十二条 系统兼容要求

乙方应确保所提供的信息系统或主要设备能够兼容 Windows7 及以上版本，所有功能和性能保持一致、稳定。

第十三条 不可抗力

因自然灾害、战争、政府指令、政府主权行为、法律变化等不可预见、不可避免、不可克服的不可抗力事件导致本合同一方当事人无法履行本合同的，受不可抗力事件影响的一方不承担违约责任，但遭受不可抗力一方因延迟履行本合同义务后遭遇的不可抗力事件除外。受到不可抗力事件影响的一方应采取措施将不可抗力事件的负面影响降到最低，否则应对对方当事人的损失扩大部分承担赔偿

责任。受到不可抗力事件影响的一方应在不可抗力发生后 2 日内书面通知对方当事人，并在不可抗力发生后 5 个工作日内向对方当事人出示不可抗力发生地有权部门出具的不可抗力事件的证明。没有在约定时间内通知对方当事人，给对方当事人造成损失的，负有通知义务的一方应承担相应的赔偿责任。

第十四条 权利义务的转让

未经甲方事前书面同意，乙方不得将其基于本合同的权利义务的全部或者部分向第三人转让，也不得用以提供担保。

第十五条 合同变更及终止

1、乙方发生以下各项的任何一种情形的，甲方无需催告等其他手续，可直接解除全部或者部分本合同。

（1） 开具的票据或者支票不能承兑，或者陷于停止支付、不能支付的；

（2） 受到监督机构停止营业或者吊销营业执照等处分的；

（3） 申请或者被申请破产、清算、拍卖等任何一种手续及与其类似的其他手续；

（4） 被第三人申请财产保全、强制执行、申请拍卖或者受到其他公权力处分；

（5） 作出解散决议的；

（6） 由于灾害、劳动争议或者其他原因，导致本合同履行困难；

（7） 发生类似前述各项导致经营困难的事由的。

2、甲乙双方可以在取得对方书面同意的情况下，解除本合同或变更本合同。

第十六条 争议解决

因本合同产生的所有争议，甲乙双方应本着诚意友好协商解决。协商无法解决时，任何一方有权向甲方所在地有管辖权的人民法院起诉。

第十七条 合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相

互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 招标文件（含招标文件补充通知）

d. 投标文件（含澄清文件）

第十八条 其他

1、本合同经甲乙双方的法定代表或授权代表签字并加盖公章后生效。

2、本合同未尽事宜，甲乙双方协商一致后签订书面补充协议。补充协议作为本合同的一部分，与本合同具有同等法律效力。

3、本合同一式 六 份，甲方执 四 份，乙方执 二 份，各份具有同等法律效力。

（本页为签字页，无正文）

甲方：首都医科大学附属北京友谊医院

（盖章）

法定代表人或授权代表

（签字）：

日期：2025 年 9 月 22 日

乙方：联通数字科技有限公司

（盖章）

法定代表人或授权代表

（签字）：

日期：2025 年 9 月 22 日

附件一：《信息系统功能需求清单》

1、 分项报价清单：

序号	分项名称	规格型号	数量	单位	单价（元）	总价（元）
1	5G边缘云管理平台-防火墙	锐捷 RG-WALL 1600	2	台	112,860	225,720
2	5G边缘云管理平台-业务接入交换机	中兴 ZXR10 5960X	2	台	145,621	291,242
3	5G边缘云管理平台-管理交换机	中兴 ZXR10 5950	3	台	14,876	44,628
4	5G边缘云管理平台-配套软件	联通云管理平台服务	1	套	146,790	146,790
5	5G边缘云管理平台-网络建设	网络建设服务（含5G专用CPE接入）	1	套	590,480	590,480
总价（元）						1,298,860

2、详细信息系统功能需求

序号	功能项	类别	功能描述
1	硬件	业务交换机	交换容量≥1.6Tbps；包转发率≥800Mpps ≥48端口万兆光口（含48个万兆光模块）+6端口40G QSFP+（含6*40GE多模模块）
2		管理交换机	交换容量≥500Gbps；包转发率≥200Mpps；48个10/100/1000Base-T以太网端口，4个万兆SFP+接口（含4个万兆多模光模块）
3		防火墙	硬件配置要求:>800Mbps，支持IPsecvpn，全新下一代千兆防火墙，1U高度，1*交流电源，固化6个万兆光口（含光模块）;1个console接口;1个USB口;RG-WAIL1600-S3200的多合授权含IPS特征库、病毒库、威胁情报、应用识别库、垃圾邮件库、网页分类库升级服务授权1年。
4	云平台	云主机	基本管理：具备单台及批量创建、删除、启动、关闭、查看虚拟化主机能力；

5			操作管理：支持控制台、API，对虚拟化主机进行基本操作、配置修改、系统重装、密码更改、实例迁移等操作的能力；
6			系统管理：至少支持麒麟、统信系统安装；具备创建前\运行中安装及重装公共镜像\私有镜像的能力；
7			配置管理：支持虚拟化主机的 CPU、内存配置调整；具备内存\磁盘容量动态调整能力；
8			密码管理：支持控制台后台及远程登录密码设置，包括普通密码\秘钥对；具备控制台修改虚拟化主机系统密码的能力；
9			迁移能力：支持虚拟化主机实例迁移，具备单实例及多实例的关机冷迁移、在线热迁移、故障自迁移（可设置）。
10			弹性伸缩：可根据通过配置伸缩组、伸缩配置、伸缩规则进行弹性扩张、弹性伸缩。
11		容器服务	集群管理：支持多集群的统一管理，包括创建、管理、升级、伸缩操作。支持多版本的原生 kubernetes 集群创建、支持自定义 kubernetes 集群默认参数修改等能力。
12			节点管理：支持节点添加、剔除、弹性伸缩等能力
13			网络管理：支持原生 kubernenetes 网络组件，支持 Calico 和 VPC-CNI 两种网络模型。具备自定义容器网段、容器安全组、服务网段能力。支持 node、pod 网段分离、独立安全组绑定能力；
14			存储管理：支持对接云盘（块存储）等；
15			监控管理：提供集群、节点、工作负载、容器组 Pod 及容器多维度的监控告警。
16		块存储	可靠性要求：提供弹性块存储，数据存储保证三副本冗余技术，保证客户高可靠性，可靠性达到 9 个 9。
17			虚拟硬盘管理：可创建空虚拟硬盘或通过快照创建虚拟硬盘，可挂载至虚拟化主机实例；支持控制台或 API 的单块或批量的虚拟硬盘创建、回收、挂载等操作；

18			虚拟硬盘快照：使用快照能力，对虚拟化主机上硬盘的快照操作，并具备快照一致性、自动快照能力。
19			高性能存储硬盘单盘最大容量要求≥30TB；
20			高性能存储硬盘单盘最大 IOPS 最大可达 20000，读写带宽≥150MB/s，并提供功能截图或官网截图等相关证明材料；
21		虚拟专有网络	基本管理：具备创建、删除虚拟专有网络实例能力
22			自定义网络：可以自定义网段，可以弹性扩展，按需划分子网，并通过灵活配置路由表和路由规则定制化部署业务；同一个私有网络支持多个自定义网段。
23			多种接入方式：可以使用普通公网 IP、弹性公网 IP、NAT 网关、负载均衡等访问 Internet；可以使用云联网、对等连接来访问其它私有网络；可以使用 VPN 连接、专线接入、云联网来访问其他数据中心；可以使用基础网络互通来访问部署在基础网络中的业务。
24			安全管理：基于隧道技术，在物理网络上构造虚拟网络，使用虚拟化技术，实现不同私有网络之间内网完全隔离；提供安全组、网络 ACL 等不同层面的网络访问控制方式。
25			弹性 IP 能力:独立的外网弹性 IP 服务，支持与虚拟化服务器、负载均衡实例、NAT 网关、弹性网卡的自绑定。具备动态调配、灵活绑定等能力
26			支持批量导入、批量导出安全组规则
27		负载均衡	基本管理：具备单\批量创建、删除负载均衡实例能力；具备绑定\解绑负载均衡后端能力
28			高可用能力：采用全冗余设计，无单点，支持同城容灾。根据应用负载进行弹性扩容，在流量波动情况下不中断对外服务。
29			多协议支持：提供四层（TCP 协议/UDP 协议）和七层（HTTP 协议/HTTPS 协议）负载均衡。
30		NAT 网关	网络地址转换：可以配置网络地址转换规则，网络地址转换（NAT）可以根据访问流方向进行 IP 转换和 IP 端口转

			换；
31			虚拟专有网内支持 NAT 网关
32		虚拟化资源管理平台	平台管理：提供独立的虚拟化资源管理平台，提供虚拟化资源的运营端和租户端服务，包含平台用户管理、消息中心、资源管理等。
33			基础设施：提供物理服务器的生命周期自动化管理，如数据导入、裸机资源发现、服务器 OS 部署、远程开关机&重启、服务器设备的监控和告警等。
34			运维平台管理：提供虚拟化资源运维平台，包含监控系统、日志平台、作业工具、巡检平台、资源概览等。
35			支持对用户设置管理范围及权限，可以指定某个用户只能看到某个特定的资源区域；
36			提供多个网络的弹性公网 IP 能力（如互联网 EIP，办公网 EIP 等），虚拟化服务器或 SLB 等资源可以根据需要，选择挂接不同网络的弹性公网 IP 实现与对应网络的互通；
37			日志管理：支持全量虚拟化产品运行日志采集，支持日志检索、日志筛选、日志导出等功能。
38			可通过统一面板展示资源、容量、告警、云资源负载、设备负载、配额等统计分析，并提供报表导出能力。
39		统一监控管理平台	告警配置：提供告警策略新增、编辑、删除能力。
40			监控管理：包括全量云平台和云产品的监控能力，包括但不限于基础资源监控（CPU、内存、磁盘容量、网络流量等）、性能监控（慢 IO、慢查询、流量堵塞等）
41			监控查询：提供监控面板，支持查询产品的运行状态信息，包括当前状态和影响对象数
42			监控告警：支持告警策略的新增、删除、修改、查询和告警模板。支持短信、邮件、站内信等多方式订阅；
43			通过自定义告警阈值配置，异常/失败等告警指标自由组合。提供历史调用趋势，供服务阈值配置。

44		平台兼容性	多芯片服务器兼容：云平台应同时支持多芯片的服务器硬件，包括海光、飞腾、鲲鹏 CPU 芯片。
45	网络	无线网络	在项目建设区域内，室外采用宏站方案进行直接覆盖或远距离覆盖，并使用覆盖能力较强的宏站产品。在宏站覆盖效果不理想区域，可根据用户实际业务需求进行区域范围内的网络优化，提升用户感知。
46			5G 专用网络应采用 SA 的组网模式，全面满足院区的无线覆盖需求，提供信号稳定、数据高效传输、网络安全可靠的 5G 无线覆盖。
47			提供的 5G 专用网络应采用工信部授权的 5G 主流频段。
48			提供的 5G 专用网络应支持 5G 网络切片，可通过 5G 切片技术将医院业务和公众业务隔离，保证医院业务数据传输的优先级。同时投标方可支持以在线的方式对切片资源进行灵活调整以及监控管理。
49			提供的 5G 专用网络应达到下行单用户速率不低于 300Mbps，下行带宽峰值速率不低于 600Mbps，上行单用户速率不低于 20Mbps，上行带宽峰值速率不低于 150Mbps，网络时延在 40ms 以内
50		核心网络	提供核心网用户面下沉部署的 5G 专用网络，设备应放置在招标方要求的机房空间内，实现院内医疗业务定向访问和数据专有链路回传存储，满足医疗数据不出医院的需求。
51			支持通过 5G 专网实现多院区间终端互联互通的需求。
52			提供具有灾备功能的 5G 专用网络，并在项目服务期内提供相应的网络运维保障服务。
53		5G 终端设备	提供具有 5G 网络 WIFI 转换功能的 5G 终端设备，满足院内非 5G 医疗终端的入网需求，并提供相应的产品质保服务。

附件二：《售后服务方案》

1、 售后服务内容

项目验收合格后，提供不少于3年的免费售后服务，包括系统维护、故障修复、数据备份和恢复等。

免费升级和维护，确保系统与医院业务发展需求保持同步。

1.1、 服务质量控制、评价和考核体系

1.1.1、 服务质量管理的主要内容

服务质量管理的宗旨是有效地利用各种资源，包括公司的资源、产品生产厂家的资源、用户资源。通过资源的优化组合，多、快、好、省地实施服务，并在实现该项目预定目标的同时，力求实现更多的附加增值功能。

该服务质量管理的内容主要有组织工作、合同工作、进度控制、质量控制、费用控制等。

1.1.1.1、 组织工作

为了确保服务的顺利实施，需要建立统一的服务质量管理组织、制定该服务项目的各项工作制度、明确相互的关系和责任、精心组织服务队伍和服务实施、组织物质供应和后勤保障等。

1.1.1.2、 进度控制

该项目既有深度又有广度。深度是指在某一节点上不同平台，广度是指不同地域的关联。因此其进度控制包括节点服务进度和不同地域的服务进度、物质供应进度、进度的协调等。整个进度控制不仅是进度计划的精心设计，而且需要计划进度和实施进度之间的协调与控制。

1.1.1.3、 质量控制

该项目所采用的硬件/软件产品不仅有相应的功能要求，而且有工业技术指标、协议标准等要求。该项目服务质量控制是建立在这些功能和指标可实现的基础上，予以全面监督和控制。在验收过程中的服务质量验收不仅是功能的实现，而且是技术指标或标准的实现。

1.1.1.4、 费用控制

该项目的费用控制，不仅是用户方或公司的费用预算和费用计划，而且是

与工程进度相配匹的投资或投入控制。

1.1.2、 服务管理的方法

1.1.2.1、 目标分解法

该项目的目标是维护医院业务安全和高效运行。针对上述目标予以服务内容、服务质量、服务计划等方面进行细化设计、计算和分解。该项目的服务管理是在上述工作基础上，对服务成本、服务质量、服务工期、安全等予以明细和规范。

1.1.2.2、 责任明确法

该项目涉及多方的参入，该项目的工程管理将对各方的责任和义务予以明确和分配。这些责任包括法律责任、义务责任、决策权责、执行权责、监督权责、提供信息的责任和义务、信息处理的责任和义务等。

1.1.2.3、 信息收集和信息反馈法

该项目服务管理中将采用标准化或规范化的工程表格作为常规的工作信息、合同信息、查询信息，通过服务进度表、工作日志、工作报告、工作会议记录等收集或反馈各种流动信息，并通过这些信息的分析、处理、决策予以工程的管理。

1.1.2.4、 协调行动法

由工程各方组成统一的工程组织，定期或不定期的举行服务管理会议、服务现场会议。每次会议、协调、通告等均予以详细的记录，其各项决定在统一的监督和管理机制下，责令相关机构执行。

1.1.2.5、 文档控制法

在实际服务过程中，采用文档的流程化、规范化的管理。文档记录服务过程中每一步具体的操作和结果。文档既是工作人员工作方法、工作成绩和工程质量的实际记录，又是工作交接、工作验收的凭证和依据。

1.1.2.6、 服务质量评价手段

公司已经通过了 ISO9001 认证。客户服务是质量管理系统的一部分。详细的介绍如下：

客户申诉管理

客户满意度测量和分析

用联合工作组和面谈来进行客户关系的管理

下表总结了客户关心和满意活动框架中调用的主要子进程。

子过程	目的
客户满意度调查	根据客户反馈来提高客户满意度和处理流程
客服管理	针对客户和的合作分析存在的问题、定义措施
客户申诉管理	修复客户的满意度和改进流程
项目相关的客户满意度调查	提高项目流程、改进项目框架

此外，为保证给用户提供最优质的服务，在内部拥有一套完备的服务质量控制程序，主要包括：《生产和服务提供控制程序》、《用户满意度测量程序》、《数据分析控制程序》、《纠正措施控制程序》，通过以上紧密衔接的从服务的提供、服务监督、量化评定，到纠正措施一整套的服务监督控制方法，保证并不断提高的服务质量，同时的工作质量评估与员工的绩效考核挂钩也为以上管理措施的执行提供了有力的保证。

2、 服务质量保证措施

2.1、 服务质量管理

服务质量是衡量项目运营及运维是否成功的标志，因此我公司项目组将建立一个完整的服务质量保证体系，从组织结构、设计、硬件采购保存、运维、调试验收、售后服务等多方面对项目建设进行质量管理。运用系统工程的观点和方法，以保证质量为目的，将有关部门、各个工作岗位、各个环节的管理和服务生产活动严密地组织起来，使全体成员形成保证质量的有机整体，落实系统运行、服务和运维三个阶段的工作内容、工作程序、权限和方法，使质量在首都医科大学附属北京友谊医院 5G 边缘云项目形成过程处于受控状态。

2.1.1、 公司质量保障体系

我公司按照 IS09001 质量保证模式建立了文件化的质量体系，它包括《质量手册》、20 个程序文件、操作层次的质量体系文件以及质量体系运行中的各种质量记录。公司文件化质量体系的建立，极大地促进了公司质量工作有组织，有秩序的开展，公司对每一项业务和每一项服务，坚持按照 IS09001 标准严格管理每一个质量环节，从合同控制、设计控制、文件和资料的控制、采购控制、设备

及过程控制，确保了每一项业务和每一项服务自始至终的过程质量处于受控状态，为最终项目质量目标的圆满实现奠定了可靠的基础。同时严格控制采购管理，对采购计划进行审批确认后，再签订采购合同，到货时进行设备检验，必要时进行性能测试，确保将最适用的产品应用到项目中。公司高度重视质量体系运行中产生的质量记录的收集、保存和管理，对质量记录格式以及从产生到归档的管理细致、严格，使之能充分反映公司质量体系运行的真实全貌，为不断开展质量改进活动提供了依据，也是实现服务项目质量可追溯性的重要依据之一。

2.1.2、 服务质量保障体系

公司现行的质量体系是公司开展各项业务活动必须遵循的总的方针和原则，而针对工程实施的服务质量管理与保证体系是公司现行的质量体系的一个具体体现，因此，它必须与公司现行的质量体系保持一致。同时，结合项目具体需求，建立实用的服务质量体系，使之有效地运行于项目实施的各个环节和阶段，以确保服务质量目标的实现。

2.2、 服务质量主要能力指标

2.2.1、 上云咨询服务能力

联通在上云咨询能力方面展现出了强大的实力和专业性，主要体现在以下几个方面：

一、丰富的上云咨询经验

联通云作为中国云计算服务市场中的重要一极，历经多年的发展，积累了丰富的上云咨询经验。不仅服务于政务、医疗等多个行业机构，还通过实际项目不断积累和优化上云咨询方案，以满足不同客户的个性化需求。

二、专业的咨询团队

联通云为首都医科大学附属北京友谊医院5G边缘云项目配置了上云咨询团队，他们具备深厚的行业知识和丰富的实践经验。咨询团队能够深入理解客户的业务需求和痛点，结合联通云的技术优势和产品特点，为客户提供量身定制的上云咨询方案。

三、全面的上云咨询服务

联通的上云咨询服务涵盖了多个方面，包括需求分析、方案设计、实施规划、风险评估等。专业的团队能够帮助首都医科大学附属北京友谊医院全面评估

上云的必要性和可行性，制定详细的上云计划，并提供全程的技术支持和指导。

四、强大的技术支持和创新能力

联通在云计算领域具备强大的技术支持和创新能力。我们不断投入研发资源，推动云计算技术的创新和发展。同时，我是还与合作伙伴共同构建生态体系，为首都医科大学附属北京友谊医院提供更加全面和优质的服务。

联通在上云咨询能力方面具备丰富的经验、专业的团队、全面的服务、场景云解决方案以及强大的技术支持和创新能力。能够为首都医科大学附属北京友谊医院提供量身定制的上云咨询方案，并助力客户实现数字化转型和升级。

2.2.2、 迁移协助服务能力

联通上云迁移能力在业界具有显著的优势和丰富的实践经验，在多个项目得到了很好的的实践。

一、定制化迁移方案

联通根据首都医科大学附属北京友谊医院的实际情况，定制化提供最适合的迁移方案。这种专属定制化的服务能够确保客户的业务在迁移过程中保持平滑过渡，减少因迁移带来的业务中断和风险。定制化方案包括网络方案，迁移方案，回退方案，验证方案等。

二、一站式交付

联通云的迁移服务具有一站式交付的特点，能够完全覆盖信息收集、评估分析、方案设计、现场实施和验收测试等业务迁移的全流程。这种全方位的服务模式能够彻底解决客户的后顾之忧，确保迁移工作的顺利进行。

三、丰富的迁移经验

联通云迁移团队自成立以来，为多个大型项目提供了迁移服务，积累了丰富的实践经验。这些经验使得联通云能够更好地理解客户的需求和挑战，并为其提供更加准确和有效的解决方案。

四、专业化的团队

联通云拥有专业化的迁移服务团队，目前团队人数达到 20 人，他们依托联通多年系统运维及上云迁移经验，提供端到端的迁移咨询及实施服务。专业的团队能够确保迁移过程的安全可靠，降低风险，并为客户提供及时的技术支持和指导。

五、多层次的迁移服务

联通云上云迁移能力不仅限于简单的数据迁移，还包括物理机迁移、虚拟机迁移等多种迁移方式。同时，联通云还提供数据迁移服务，以满足客户的多样化需求。

六、合规性与安全性

在迁移过程中，合规性和安全性是至关重要的。联通云严格遵守国家相关法律法规和行业标准，确保迁移过程的合规性。同时，联通云还具备强大的安全能力，能够为客户提供全方位的安全保障，确保客户的数据和业务在迁移过程中不受任何威胁。

联通具备上云迁移及定制化的一站式交付能力、拥有丰富迁移经验和专业化团队。

2.2.3、 网络巡检能力

对于中国联通为客户所提供的各类 5G 通信设施，中国联通将会制定相应的维护作业计划，对客户端网络设备进行巡检，发现问题应及时反馈并处理，同时提供《网络运行分析报告》，以保障设备的安全可靠运行

中国联通在完成设备部署及试运行之后，需提供详细验证报告，报告中需包含招标文件中的验收项，注明各项测试数据，与验收标准作对比验证是否达标，并保证在各场景下好点数量大于 85%，中点数量大于 13%，差点数量控制在 2%以内。

若存在不达标项，需在 3 个工作日内完成整改，若延期处理，需提供书面情况说明并交由客户相关部门进行确认。

2.2.4、 服务人员能力

本项目联通投入的运维服务人员的能力主要体现在以下几个方面：

一、专业技能

云计算技术：运维服务人员具备深厚的云计算技术基础，包括云平台的架构设计、部署、运维等，以确保灾备中心系统的稳定运行和高效管理。

网络安全：在云环境中，网络安全至关重要。运维服务人员熟悉各种网络安全技术和策略，能够有效应对网络攻击和数据泄露等风险，保障数据的安全性和完整性。

IT服务管理：运维服务人员掌握IT服务管理的相关知识和技能，包括服务级别管理、问题管理、变更管理等，以确保云服务的连续性和可靠性。

二、业务能力

行业知识：服务人员了解相关行业的业务流程、政策法规和特殊需求，可以更好的为客户提供定制化的云服务解决方案。

需求分析：运维服务人员具备出色的需求分析能力，能够准确理解客户的需求和痛点，为其提供符合实际的云服务建议和优化方案。

项目管理：在项目实施过程中，运维服务人员具备项目管理能力，包括项目计划制定、进度控制、风险管理等，以确保项目按时按质完成。

三、沟通与协调能力

客户沟通：运维服务人员具备良好的沟通能力和客户服务意识，能够与客户保持密切沟通，及时响应客户需求和反馈，提供优质的服务体验。

内部协作：在运维服务团队中，服务人员具备与其他团队成员紧密协作，共同解决技术难题和客户需求，确保团队目标的顺利实现。

四、持续学习与创新能力

持续学习：云计算技术发展迅速，运维服务人员保持持续学习的态度，不断跟踪新技术和新趋势，提升自己的专业技能和业务能力。

创新能力：服务人员具备创新思维和创新能力，能够针对客户的特殊需求提出创新性的解决方案，推动云服务的不断升级和优化。

2.3、 服务质量保证措施

2.3.1、 计算存储资源服务质量

一、资源弹性伸缩

本项目，联通提供自动化的资源管理和弹性伸缩能力，确保客户可以根据实际需求动态调整计算和存储资源，避免资源浪费或不足的情况。

二、数据冗余与备份

采用数据复制和备份策略，确保数据的持久性和安全性。本项目块存储使用三副本数据冗余方案，防止数据丢失。

三、灾难恢复计划

制定详细的灾难恢复计划，每年进行灾难恢复演练，确保在发生重大事件

时能够快速恢复服务。

四、性能监测与预警

实施全面的性能监测和预警系统，实时监控资源使用情况，及时发现并处理潜在问题，避免影响用户体验。

五、服务质量协议（SLA）

提供明确的服务水平协议，承诺一定的服务可用性和响应时间，按照 99.99%或更高的可用性指标执行，并在不达标时给予补偿。

六、技术支持与客户服务

设立专门的技术支持团队，提供 7x24 小时的运维支持和咨询服务，确保用户遇到问题时能够得到及时解决。

七、网络安全防护

强化网络安全措施，包括防火墙、入侵检测系统、DDoS 防护等，保护数据免受外部威胁。

八、持续优化与创新

九、不断优化现有的服务架构和技术，引入最新的云计算技术，提升整体的计算和存储效率。

十、服务器稳定性保障：部署高品质、高可靠的服务器设备，采取冗余配置，确保服务器的高稳定性和可用性。

十一、高性能存储设备：采用高性能存储设备，如固态硬盘（SSD），提高数据读写速度，减少用户响应时间。

十二、双电源供电：为服务器设备提供双电源供电，防止单电源失效带来的服务中断。

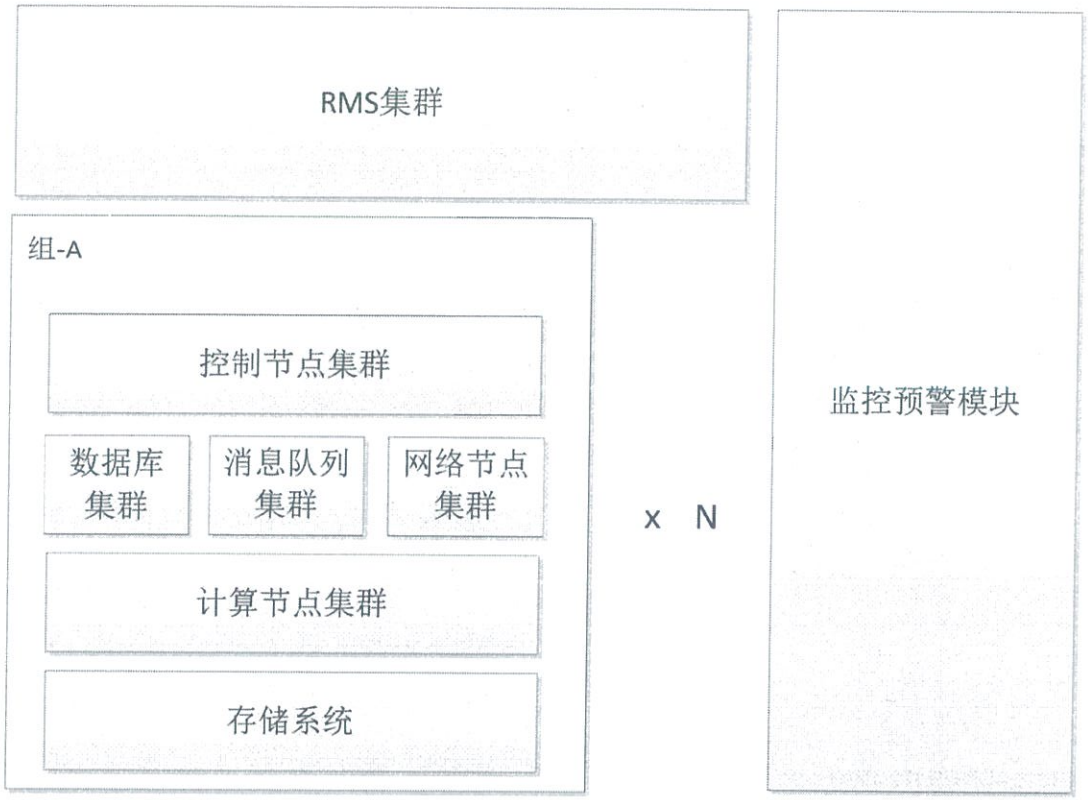
十三、温湿度控制：通过实施温湿度控制，保持服务器的稳定工作环境，提高设备的运行效率和寿命。

具体底层实现方式如下：

计算体系属于 Iaas 体系中的子系统，向上接 RMS 子系统调用，与网络子系统、存储子系统并列提供基础设施服务。

计算体系以单个组（group）为部署单位，由 RMS 体系统一管理多个单位组，并可以动态注册或注销某个单位组；在单个组内划分为控制节点、计算节点、消息队列、数据库、网络服务五类集群，每类集群可以动态增加节点满足可扩展性和

可靠性的需要，每个组内共享一套存储共享文件系统；计算体系的监控告警信息由监控模块统一提供，该模块服务于整个平台，也是 Iaas 平台实现集群等功能的必要条件，整体逻辑结构如下图：



整体拓扑图

根据计算体系中各部分的功能，将整个系统划分为五个模块，分别为：

- API模块（API）
- 调度模块（scheduler）
- 计算模块（compute）
- 镜像模块（glance）
- 认证模块（keystone）
- 可靠消息队列（AMPQ）

- API 模块

API 模块是计算体系的统一对外接口，提供 HTTPWebService 形式接口，主要处理身份验证和授权，以及基本的命令和控制功能，默认情况下 API 模块监听 8774 端口。接受并履行 API 请求，也将强制执行一些策略（主要是身份验证，授权和配额检查）。对于一些要求，API 模块会完成整个请求，通过查询数据库，

然后返回结果；对于更复杂请求，它向数据库写入相关信息，并投递消息到消息队列中。

- 调度模块（scheduler）

调度模块（scheduler）在 openstack 中的作用就是决策虚拟机创建在哪个主机上，目前调度仅支持计算节点，调度的依据来自于数据库信息和各计算节点定时上报的资源信息。

调度模块的子模块包括：

- 过滤模块

通过调度信息过滤出一批合适的计算节点；

- 权重模块

在过滤模块筛选出的计算节点中依据权重指标定位一台计算节点；

认证模块（keystone）

认证模块（keystone）包括以下组件

- keystone 包含一个命令行接口，可以与 KeystoneAPI 交互以管理 keystone 和相关服务。
- keystone-admin-操作 keystone 的管理 API
- keystone-service-用于验证的，面向用户的 AP
- keystone-manage-管理 keystone 的命令行接口
- keystone 还包括 WSGI 中间件为 Nova 和 Swift 提供验证服务。
- keystone 使用一个内置的 SQLite 数据库-为验证用户，将来也可能使用一个外部 LDAP 服务来代替存储证书

1） 镜像模块（glance）

Glance 提供镜像服务，后端可以对接 S3、RBD、Swift 等存储介质；镜像模块有两个 WSGI 服务模块。

- Glance-API：主要负责接收响应镜像管理命令的 Restful 请求，分析消息请求信息并分发其所带的命令(如新增，删除，更新等)，默认绑定端口是 9292。

- Glance-Registry：主要负责接收响应镜像元数据命令的 Restful 请求。分析消息请求信息并分发其所带的命令（如获取元数据，更新元数据等），进行数据库相关的增删改查工作。默认绑定的端口是 9191。

子模块

计算模块是直接操作虚拟机的模块，也是通常计算节点上的唯一模块。由以下几个子模块构成：

负责监听和接收指定的消息队列，对任务进行初步处理并下发 Driver 模块；

负责调用 quntumclient 和 cinderclient 与网络、存储子系统进行交互；

Manage 子模块同样负责将 driver 子模块采集到的信息汇报给调度模块；

Driver 模块提供统一接口，并根据配置文件的选项路由到不同的 driver 包，对于不同的虚拟化类型执行操作，目前主要支持 kvm 和 vmware 两种虚拟化类型；

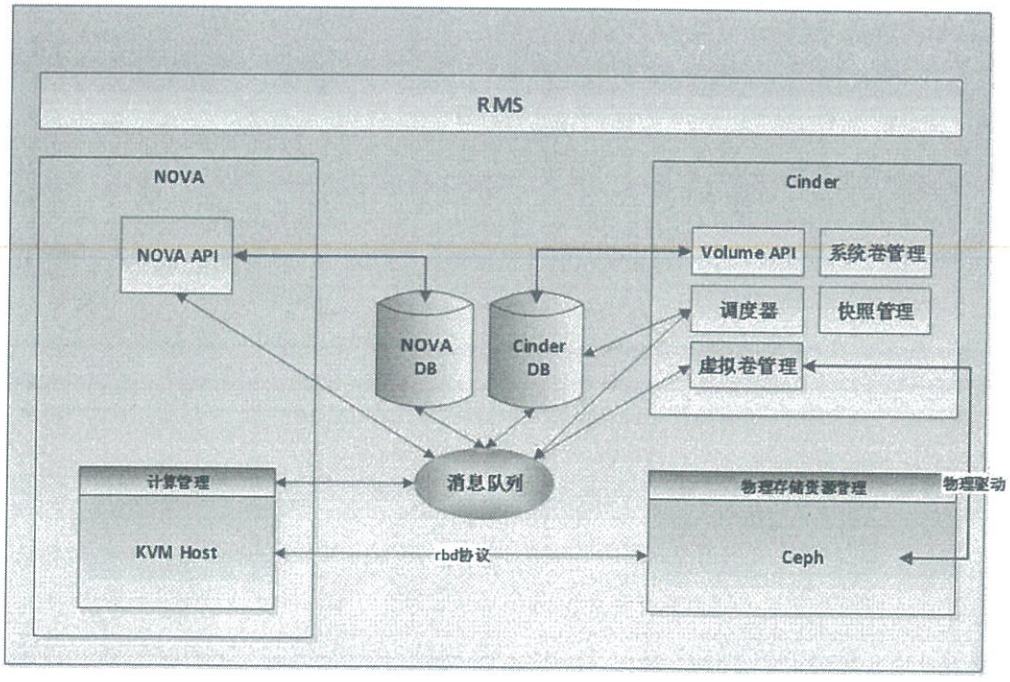
提供通用工具类供 driver 调用；

计算服务质量保证：

定期检查子系统内的服务，包括 API、调度、认证、镜像服务和计算服务的工作状态。以检查计算服务为例，涉及内容包括：检查计算模块运行状态、查询虚拟机列表、镜像模块监测等。系统维护操作示例云平台计算资源管理子系统，可以对虚拟机的生命周期进行管理，包含创建、启动、查看、停止、销毁等。同时，可以对镜像进行创建、上传和销毁等管理。

云平台存储资源管理子系统 Cinder，它为虚拟机(VM)提供了持久块存储。对于可扩展的文件系统、最大性能、与企业存储服务的集成以及需要访问原生块级存储的应用程序而言，块存储通常是必需的。

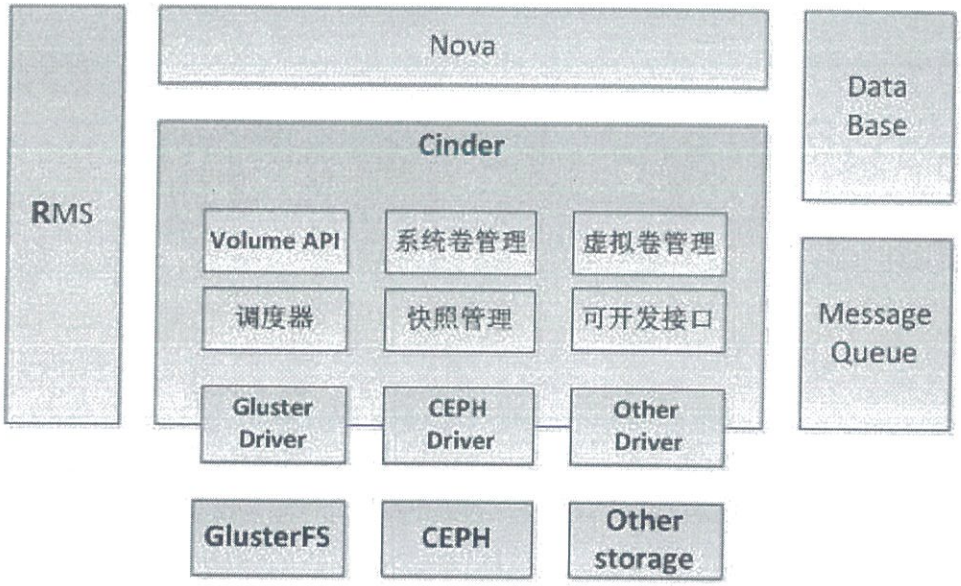
存储子系统模块在整个 IaaS 架构的位置如下图。



存储子系统架构

如图所示，存储系统模块为整个 IaaS 提供存储服务，这些服务包括：为管理节点提供镜像与模板存储服务；为计算节点提供实例存储服务；为虚拟机系统卷提供查询服务；为虚拟机提供数据卷添加、删除、挂载、卸载、快照等服务；为虚拟机提供备份还原服务。

存储子系统 Cinder 主要为虚拟机提供数据卷添加、删除、挂载、卸载、快照等服务，其体系架构如下：



Cinder 体系架构图

Cinder 模块通过 RMS 系统进行管理配置，并向 Nova 系统提供虚拟机数据卷创建、删除、快照、加载、卸载等服务。

Cinder 底层支持多个存储的 Driver，包括 Gluster、Ceph 等分布式文件系统的 Driver；或者一般 IPSAN、FCSAN 等块存储的 Driver；或者 NETAPP 等 NFS（NAS）的 Driver。有了这些 Driver 以后，Cinder 模块就可以屏蔽底层存储的各种差异，对上层 nova 层提供统一的操作接口。

存储服务质量保证

通过指令检查 cinder 工作状态；

登录每台计算节点，检查与共享存储连接状态

检查共享存储健康状态与性能参数

检查挂载点、存储网络健康状态、存储服务状态

检查 glusterfs 挂载状态

2.3.2、 网络资源服务质量

全国多级算力资源布局：联通云落实国家“东数西算”战略，采用“5+4+31+X”架构进行全国多级算力资源布局，构建“1+N+X”智算能力布局，实现多样性算力一体化供给。这一布局有助于优化网络传输路径，减少网络延迟，提高数据传输效率。

高效协同一体化的全光算力传输网：联通云打造了高效协同一体化的全光算力传输网，实现算力网络全光化、低时延、大带宽、高可靠。这种网络架构能够支持多层级算力布局，覆盖“东数西算”场景，为用户提供高质量的云内网络服务。

主要服务质量体现在以下几个方面

高带宽与低延迟：联通云通过增加带宽和处理能力，提高数据传输效率和稳定性。同时，采用 CDN（内容分发网络）等技术，将数据分发到离用户更近的节点，减少传输时延。这种技术优化有助于提升云内网络的整体性能。

弹性与可扩展性：联通云网络资源支持弹性扩展，能够根据用户业务需求自动调整资源分配，确保云内网络在高并发场景下的稳定性和可用性。这种弹性扩展能力有助于用户应对业务波动和突发情况。

多线接入：建立多个接入点，通过多个网络运营商接入，确保网络的稳定性和可靠性。

带宽扩展：增加网络带宽，满足用户对大数据传输、高并发访问等需求，保证用户在高峰期的服务质量。

DDoS 攻击防护：部署 DDoS 攻击防护设备，对 DDoS 攻击进行实时监控和阻断，保护用户的服务不受攻击影响。

网络安全体系与加密认证：联通云建立了完善的网络安全体系，采用先进的加密和认证技术，确保客户数据的隐私和安全。同时，加强对云计算平台的监控和审计，及时发现和防范安全威胁，保障云内网络的安全性。

专属网络 VPC 服务：联通云提供 VPC（专有网络）服务，为用户提供一个隔离、安全的网络环境。VPC 服务通过链路冗余、网关主备等多种技术保障网络高可用性和安全性，确保云内网络数据的传输安全。

服务与支持

全天候服务保障：联通云提供 24 小时网络运行监管和客户服务，及时检测网络

异常并为用户提供解决方案。这种全天候的服务保障有助于用户快速解决云内网络问题，确保业务连续性。

联通云计算的云内网络服务质量在网络架构、性能稳定性、安全性与隐私保护方面有着出色的服务质量。

云平台网络资源管理子系统 Neutron 实现 IaaS 系统中虚拟网络管理、IP 地址分配、虚拟网络设备的管理，虚拟网络设备的访问控制以及 IaaS 系统内的虚拟设备与外部网络之间的相互访问。

Neutron 组件包括 Server、Dhcp-agent 和 Openvswitch-agent 三个功能模块。Server 模块对外通过 Http 方式提供 Restfull 风格的接口，提供包括虚拟网络管理、IP 地址管理、虚拟网络设备管理、虚拟网络设备的访问控制管理和网络映射管理服务;对内向 Dhcp-agent 和 Openvswitch-agent 提供 RPC 调用的方式提供信息查询。Server 模块通过消息通知机制控制 Dhcp-agent 模块来实现虚拟网络设备的 IP 地址分配功能;通过消息通知机制控制 Openvswitch-agent 模块来实现虚拟设备的访问控制模功能、带宽设置。

根据系统各部分的功能，将整个系统划分为三个顶层模块，分别为：Server 模块、Dhcp-agent 模块和 Openvswitch-agent 模块。

系统模块划分

1、Server 模块

接收 API 请求

数据库操作

向 Dhcp-agent 模块发送消息

向 Openvswitch-agent 模块发送消息

处理其它模块的 RPC 调用请求

2、Dhcp-agent 模块

处理 Server 模块发送的消息

控制 Dhcp 服务器 dnsmasq

完成 iptables 操作

3、Openvswitch-agent 模块

处理 Server 模块发送的消息

操作 openvswitch，完成虚拟网络访问控制功能

操作 openvswitch,完成虚拟网络流量限制功能

Neutron 中各个模块之间利用 MessageQueue 交互信息。

各模块交互关系

网络服务质量保证

云平台网络资源管理子系统负责虚拟网络管理、IP 地址分配、虚拟网络设备的管理，虚拟网络设备的访问控制以及 IaaS 系统内的虚拟设备与外部网络之间的相互访问管理。

运维内容包括虚拟网络的查询、创建、绑定、解绑与删除；IP 地址的分配、虚拟网络设备的管理，虚拟网络的访问控制以及虚拟设备与外部网络之间的相互访问管理。

通过指令，运维常见操作如下：

查询网卡信息

查询网卡状态；

查询安全组状态；

查询公网 ip 状态

查询公网 ipnat

查询 vm 端口组

根据公网 ip 反查 vm 信息

测试存储网络 I/O

cos 删除公网 ip

查询路由器/vm 的转发规则

修改 vm 带宽

负载均衡查询与变更工作模式

LB 删除不完整引起网络访问异常

底层命令添加转发规则（端口 nat 映射）命令。

2.3.3、 安全资源服务质量

数据加密：采用先进的加密技术，对数据进行加密处理，保护用户数据的机密性和完整性。

访问控制：通过访问控制机制，对用户的身份进行认证和授权，确保只有授权用户可以访问和操作数据。

数据备份与恢复：定期备份用户数据，并建立容灾备份设施，以防止数据丢失和意外情况发生时能够迅速恢复数据。

容灾备份保障：

备份设备：建立完善的备份设备，将用户的数据进行备份存储。

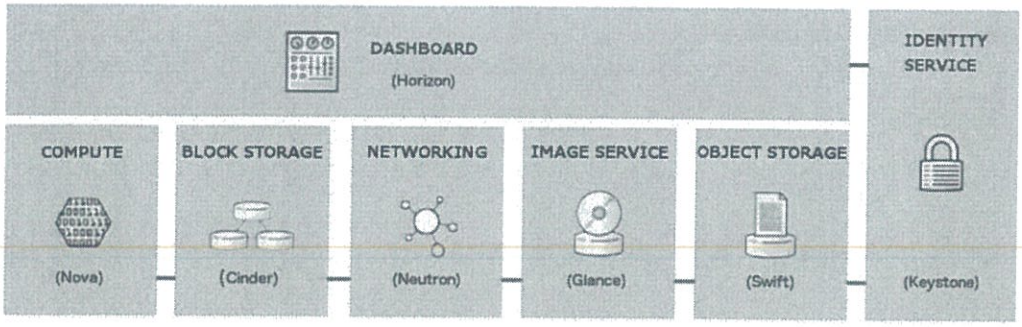
备份策略：制定合理的备份策略，根据用户需求和数据敏感程度，设定备份频率和备份存储周期。

容灾机房：在不同地理位置建立容灾机房，确保即使发生灾难性事件，也能迅速切换到备份设备，保证用户的服务不中断。

云平台资源池云安全管理子系统包括以下几个安全方面：Keystone 认证服务、安全通信机制和资源隔离。

Keystone 认证服务

Keystone（OpenStackIdentityService）是 OpenStack 框架中，负责身份验证、服务规则和服务令牌的功能，它实现了 OpenStack 的 IdentityAPI。Keystone 类似一个服务总线，或者说是整个 Openstack 框架的注册表，其他服务通过 keystone 来注册其服务的 Endpoint（服务访问的 URL），任何服务之间相互的调用，需要经过 Keystone 的身份验证，来获得目标服务的 Endpoint 来找到目标服务。Keystone 在 OpenStack 中的位置如下：



Keystone 在 openstack 中的位置

Keystone 基本概念介绍

User:User 可简单的理解为用户,用户携带信物(token)能够访问 openstack 各个服务和资源。

Tenant：Tenant 即租户，早期版本又称为 project，它是各个服务中的一

些可以访问的资源集合。比如通过 nova 创建虚拟机时要指定到某个租户中，在 cinder 创建卷也要指定到某个租户中。用户访问租户的资源前，必须与该租户关联，并且指定该用户在该租户下的角色。

Role：Role 即角色，可以理解为 VIP 等级，用户的 Role 越高，在 openstack 中能访问的服务和资源就更多。

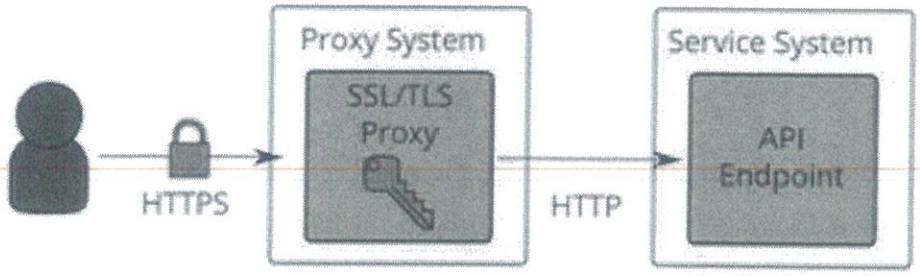
Service：Service 即服务，如 Nova、Glance、Swift、heat、ceilometer 等。Nova 提供云计算的服务，Glance 提供镜像管理服务，Swift 提供对象存储服务，heat 提供资源编排服务，ceilometer 则是提供告警计费服务，cinder 提供块存储服务。

Endpoint：Service 的显得太抽象笼统。Endpoint 则具体化 Service。Endpoint 翻译为“端点”，我们可以理解它是一个服务暴露出来的访问点，如果需要访问一个服务，则必须知道他的 endpoint，而 endpoint 一般为 url，我们知道了服务的 url，我们就可以访问它。Endpoint 的 url 具有 public、private 和 admin 这三种权限。publicurl 可以被全局访问，privateurl 只能被局域网访问，adminurl 被从常规的访问中分离。

Token：Token 即是信物、令牌，用户通过用户名和密码获取在某个租户下的 token，通过 token，可以实现单点登录。

Credentials：该术语可以简单的理解为用户和密码。

安全通信：SSL/TLS 协议是网络安全通信的重要基石，OpenStackHTTP 服务利用 SSL/TLS 实现网络安全。



安全通信

资源隔离：OpenStack 支持多租户技术，多租户技术是云计算中一种软件架构技术，旨在解决如何在多用户的环境下（比如云计算环境）共用相同的系统或程序组件，又确保各用户间数据的隔离性。在多租户技术中，租户（Tenant）是指使用系统或计算资源的用户，包含在系统中可识别为指定用户的一切数据，比

如在系统中创建的账户与统计信息（AccountingData），以及在系统中设置的各式数据和用户所设置的客户化应用程序环境等，都属于租户的范围。

OpenStack 结合多租户技术、虚拟化技术、SDN 技术、SDS 技术等实现存储、计算和网络等资源的隔离。

安全服务质量保证

云平台资源池安全管理子系统的运维方案设计如下：

云平台资源池安全管理子系统依靠 keystone 模块来实现安全管理功能。运维工作围绕 keystone 开展。日常运维中定期备份 keystone 数据库，检查 keystone 服务运行情况等。

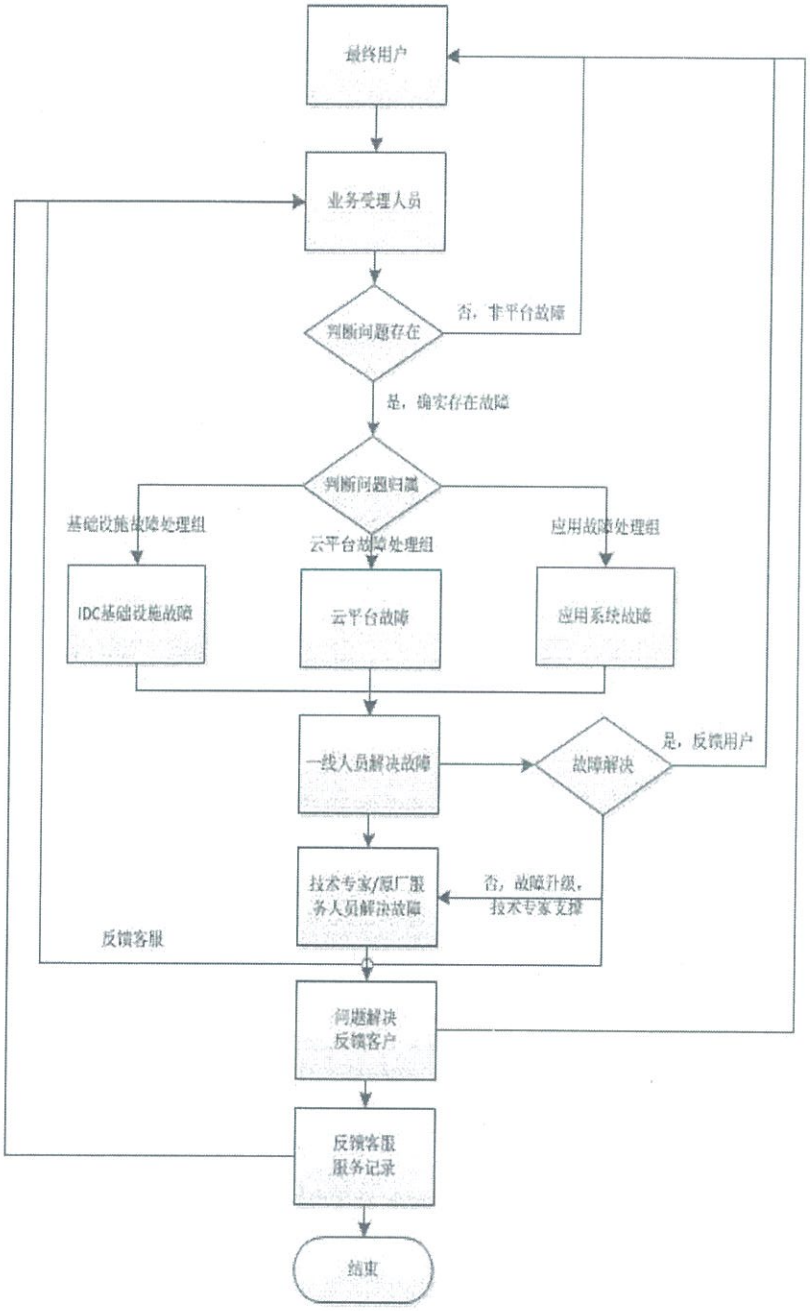
2.3.4、 事件时间处理与响应质量

云服务的服务质量和保障是联通通过一系列措施和方法来确保的。这些措施涵盖了硬件设备、网络设施、数据安全、容灾备份以及监控与维护等多个方面，旨在为该项目提供稳定、安全、高效的云服务体验。

2.3.5、 响应管理规范

我公司结合运行保障与服务运维体系，为云平台用户提供运行保障与服务运维流程。对于事件处理都进行记录，并生成处理日志可供追溯。

（一）处理流程



（二）事件受理

(1) 电话咨询

对于用户维护类和一般故障类问题，我公司维护工程师提供咨询接收服务和咨询受理服务，尽最大努力，最大限度满足需求。

客户支持中心设立热线服务电话，每周 7 天，每天 24 小时提供电话咨询服务。

电话咨询的问题能根据技术文件解决一般性操作维护问题，一般不需要进行进一步的技术调查，包括：

一般问题咨询

产品咨询

硬件咨询

软件咨询

数据咨询

版本咨询

维护经验咨询

(2) 电话支持

用户在维护系统过程中，遇到使用中的疑难或者自己不能解决的技术故障时，可通过电话或邮件的方式向我公司提出服务请求。也可以通过项目直属的项目经理提出服务请求。

客户支持中心接到技术支持的服务请求后，将首先通过电话支持服务进行响应，根据故障现象划分故障的等级，在规定的时间内通过电话帮助客户进行故障定位，并提出解决方案，最终指导客户排除设备故障。

电话支持服务为7×24小时方式。

(3) 网上值班

用户在维护系统过程中，遇到使用中的疑难或者自己不能解决的技术故障时，可通过邮件（hqs-pscwocloud@chinaunicom.cn）的方式向我公司提出服务请求。客户支持中心接到技术支持的服务请求后，将首先通过电话支持服务进行响应，根据故障现象划分故障的等级，在规定的时间内通过电话帮助客户进行故障定位，并提出解决方案，最终指导客户排除设备故障。

(4) 远程技术支持

对于通过电话支持服务项目不能解决的故障，我公司在征得用户同意后，可以通过远程服务网络，登录到服务器，进行故障诊断，查找故障出现的原因，指导用户处理故障。

为了保障用户网上设备的安全，我公司在远程技术支持过程中，只通过远程登录手段进行故障诊断和设备状态查询，而不向设备增加、更换和删除任何软件、技术参数、数据等。

(5) 现场技术支持

对于通过电话支持服务和远程技术支持服务都不能解决的故障，我公司将

迅速提供现场支持服务，安排经验丰富的维护工程师赴现场分析故障原因，制定故障解决方案，助排除故障。

(6) 软硬件升级支持

联通云的软硬件升级方案通常围绕提升其云服务的性能、安全性、兼容性和用户体验进行。以下是一些基于联通云公开信息概括的升级要点：

- 操作系统升级：联通云推出了自主可控的操作系统版本，支持云原生和虚拟化双技术栈，能够全面适配主流的国产软硬件环境，确保系统的稳定性和安全性。
- 算力提升：联通云致力于成为“算力引擎”，通过升级硬件设施，引入新一代算力技术体系，提升整体的计算能力和效率。
- 场景云服务：联通云针对不同的业务场景提供定制化的场景云服务，满足用户单位多样化的算力需求。
- 生态认证与合作：联通云积极与主流国产化软硬件厂商实现互认证，构建产业生态链，并提供系统迁移工具，帮助企业平滑过渡至新的云环境。
- 固件升级：针对特定用户，如联通用户，提供专用的固件升级服务，确保设备的最新状态和最佳性能。
- 安全可靠：升级后的联通云强调安全可控，通过多种安全机制保障用户数据的安全。
- 多云协同：联通云支持多云环境下的协同工作，让用户能够在不同云平台间灵活选择和切换。

(7) 事件处理

由各个系统运维团队值班人员负责提取工单（实时，值班人员需保证工单系统一直处于在线状态），根据工单的描述，再次进行判断，也分为三种情况：

1. 通过调整设置能解决，无需总部/原厂专家技术支持；

2. 免责，即非我公司原因造成，是客户自身应用系统或者操作造成的；

3. 需要总部技术专家或原厂技术专家支持。

对于情况 1，维护组值班人员应立即处理，处理后应测试，测试没有问题，立即回复相关运维服务团队值班人员，即时由相关运维服务团队值班人员直接回复客户以确认，同时，相关运维服务团队值班人员回复申告渠道并同时记录处理

过程，归档。

对于情况 2，相关运维服务团队值班人员应及时与客户沟通，尽最大能力协助客户，如确实无能为力，应记录描述，留存相关材料，并反馈给相关运维服务团队管理人员，同时反馈相关运维服务团队值班人员，由相关运维服务团队值班人员与客户进行最终确认。

对于情况 3，相关运维服务团队值班人员应将事件转给二线技术专家服务人员，由相关专家部门指定处理人。此时，相关运维服务团队值班人员除根据紧急程度定时向技术专家询问处理进展，还需与相关运维服务团队值班人员保持根据紧急程度而确定的频度联系。所有联系应在系统中留有处理记录。如技术专家反馈已经解决，则进入事件解决流程。

(8) 事件解决

运维服务团队值班人员根据反馈情况及时进行验证测试。事件确实解决，应即时反馈给相关运维服务团队值班人员，由其反馈给申告渠道以及客户。相关运维服务团队值班人员编写处理报告，相关运维服务团队值班人员则在系统做好处理记录，归档处理。报告及处理记录需告知相关运维服务团队管理人员。最后相关运维服务团队管理人员要形成资料库并保存在公共学习文档中，便于总结维护经验。

附件三：《运维服务方案》

1、 运维服务内容

提供本项目软件的基础软件运维服务，服务以远程方式提供，具体内容包括云业务开通支撑、云平台故障处置、故障报告出具、5G 网络日常运维支撑等。

1.1、 云平台运维保障服务

针对本项目我公司提供的云平台运维保障是通过实时资源监控（覆盖计算、存储、网络及容器集群状态）、主动安全防护（端到端加密传输、漏洞扫描与防火墙策略优化）、故障分级响应及数据全生命周期管理，确保系统高可用性、业务连续性及数据主权合规，同时依托季度健康巡检与动态性能调优实现资源利用率提升与运营成本压降，最终赋能医疗核心业务场景零中断运行。

1.1.1、 云平台运营管理

1.1.1.1、 日常运营管理作业

按要求执行日常运营作业计划，对现网资源池进行巡检及预防性维护，并做好相关记录。日常运营作业包括：

1. 检查和记录云平台资源池的平台模块及各项服务运行状态指标，保证该系统运行状态正常。并形成巡检文档，按要求上报相关主管和存档形成知识库。巡检内容涉及：云平台模块及各项服务运行状态监测，关键配置文件及组件服务状态监测，使用脚本巡检系统关键服务状态等；
2. 定期备份所有数据库文件，数据库管理维护，管理维护 Web 站点服务器、数据库服务器的备份、同步各地数据，预防、处理突发事件，制订安全规则；
3. 资源池硬件网络设备和客户虚拟网络设备的运行维护；
4. 协助排查客户虚拟网络及虚拟网络设备方面故障；
5. 定期备份物理网络设备和虚拟网络设备的配置文件，包含路由表、配置文件、ACL 访问规则；
6. 定时巡检各资源池网络设备及客户虚拟网络设备工作健康状况，发现异常及时上报并跟踪处理；
7. 云平台安全设备的巡检、维护和异常日志分析；

1.1.1.2、 安全保密制度

1. 云平台维护人员出入机房应佩戴工作证件，进入机房应着防静电工作服、工作鞋。机房应执行安全保卫管理规定，外来人员不得擅自进入机房。外部人员因公

进入机房，应经上级批准并由有关人员带领方可入内，如须携带与工作相关物品的，需要将所携带物品作详细登记。外籍人员因工作需要进入机房，须严格履行涉外手续，经运维管理部门领导批准后，指定中方陪同人员并详细记录进出机房人员的姓名、时间、批准人及工作情况。

2. 云平台维护人员应遵守动力维护部门的相关制度与管理规定，非专业人员禁止对动力设备进行操作，发现问题应立即通知动力维护部门。当机房的交流供电系统全部停止工作时，维护人员应立即向运维管理部门报告，并采取必要措施保证设备安全。

3. 各级维护和管理人员，均应熟悉并严格执行有关安全保密规定，签署保密协议。云平台的所有员工要有高度的职业道德素质，对用户在机房使用的各种资源信息及资料要严格保密，不能泄漏给任何其他人员。网络运行维护部门应定期检查安全保密制度执行情况。

1.1.1.3、 割接管理

因工程施工、网络建设、网络优化、节点扩容等原因，需要进行网络割接，原则上客户经理提前一周通知客户，明确影响业务清单，客户确认割接时间后方可实施。

对由于不可控因素如市政建设、桥路迁改、自然灾害等引起的光缆、电缆等线路紧急割接，由运维部门将割接信息提前通知客户，尽量保证不影响业务的正常进行。

对于不影响业务的割接升版，原则上提前 3 个工作日提交申请及割接方案，对于影响业务的割接原则上提前 5 个工作日提交申请及割接方案。

割接方案应至少包括以下内容：

1. 割接目的、背景。

2. 割接时间和人员安排。

3. 割接实施步骤：包括割接前准备工作和具体执行步骤，需明确到各执行步骤的执行时间、人员和具体操作。

4. 测试方案。

5. 回退方案：明确回退原则、时间、回退步骤。

6. 割接影响范围。

7. 需要配合的事项：明确数据中心内外需配合的部门及配合工作。

8. 应急预案：认真分析割接后可能出现的问题，并给出应急处理方法。

1.1.2、 云平台安全保障

1.1.2.1、 安全保障体系

完善的安全保障体系，需要完善的运营管理来支撑。安全服务专家团队凭借深厚的行业安全服务经验，并参照业界最佳实践为用户提供专业、可信、性价比高的信息安全运维服务，内容包含检测评估——>防护加固——>监控响应——>审计追查，为云平台提供从安全加固，到日常运维和应急响应完整的服务流程。客户可以根据自身具体情况，选择相应服务组件或具体设计的个性化运维服务方案，并可选择一次性服务或每年 4 次、6 次、12 次等不同的服务频率。

一、应急响应

紧急事件响应，是当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。

紧急事件主要包括：

病毒和蠕虫事件

黑客入侵事件

误操作或设备故障事件

但通常在事件爆发的初始很难界定具体是什么。所以，通常又通过安全威胁事件的影响程度来分类：

单点损害：只造成独立个体的不可用，安全威胁事件影响弱。

局部损害：造成某一系统或一个局部网络不可使用，安全威胁事件影响较高。

整体损害：造成整个网络系统的不可使用，安全威胁事件影响高。

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查。因此对于客户紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。

二、识别事件

在指定时间内指派安全服务小组去负责此事件

事件抄送专家小组

初步评估，确定事件来源

注意保护可追查的线索，诸如立即对日志、数据进行备份（应该保存在磁带上或其它不联机存储设备）

联系客户系统的相关服务商厂商

三、缩小事件的影响范围

确定系统继续运行的风险如何，决定是否关闭系统及其它措施

客户相关工作人员与本公司相关工作人员保持联系、协商

根据需求制定相应的应急措施

四、解决问题

事件的起因分析

事后取证追查

后门检查

漏洞分析

提供解决方案

结果提交专家小组审核

五、后续工作

检查是不是所有的服务都已经恢复

攻击者所利用的漏洞是否已经解决

其发生的原因是否已经处理

保险措施，法律声明/手续是否已经归档

应急响应步骤是否需要修改

生成紧急响应报告

拟定一份事件记录和跟踪报告

事件合并/录入专家信息知识库

1.1.2.2、 安全培训

技术培训主要是提高员工的安全意识和安全技能，使之能够符合相关信息安全工作岗位的能力要求，全面提高客户整体的信息安全水平。

针对不同层次的员工，进行有关信息安全管理的理论培训、安全管理制度培训、

安全防范意识宣传和专门安全技术训练，确保组织信息安全策略、规章制度和技术规范的顺利执行，从而最大限度地降低和消除安全风险。

安全意识培训

通过对客户全体员工的安全培训和工作，提高全体工作人员的信息安全意识和技术水平，降低由于人为原因引发的安全风险。

管理类培训

针对客户不同层面、不同职责、不同岗位的人员进行培训，在客户方内部推行、实施已建立的安全体系，提高信息安全管理水平。

安全流程制度培训

针对相关的安全流程、安全制度、安全规范、安全运维计划进行培训，使员工了解相关的、系统级的安全体系操作流程和制度。

1.1.2.3、 系统上线检测

系统上线前检测是应用系统生命周期中的一个重要环节，在对应用系统建设规划和现状充分调研的基础上，制订系统上线前的安全检测方案，并根据信息系统平台建设情况，按照系统上线前安全检测方案实施检测工作，进行彻底全面的安全弱点评估，发现潜在的安全漏洞。上线前检测需采用对系统非侵害的测试方法，检验系统的安全防护能力，发现安全风险及漏洞，采用方法至少包括远程渗透测试、设计文档检查等。

通过上线前的检测工作，对应用系统所覆盖的全部资产再次进行确认识别，完成对应用系统等级保护建设措施落实情况的合规性分析，对应用系统等级保护实施的各项安全措施和管理制度进行全面的风险评估，明确残余风险；依据风险评估结果、上线前检测结果、合规性分析结果，进行差距分析，提出安全改进建议。

各级维护和管理人员，均应熟悉并严格执行有关安全保密规定，签署保密协议。云平台的所有员工要有高度的职业道德素质，对用户在机房使用的各种资源信息及资料要严格保密，不能泄漏给任何其他人员。运行维护部门应定期检查安全保密制度执行情况。

云平台运维管理人员的工作内容包括：

提供辅助上云服务，包括上云咨询和评估、上云解决方案设计、实施，以及上云后技术支持服务，降低上云技术风险和资源成本；

提供云服务稳定保障服务，实施云服务高可用自检的通用检查内容及指导，检查可用性风险，并针对项目云服务进行各服务可用性风险排查；

提供云服务安全辅助服务，包括提供应用上云安全部署、安全设备保障、安全漏洞扫描、安全事件响应、安全评测复审服务，为客户提供云平台层面安全保障，同时协助客户培养安全用云意识和操作习惯；

提供全面的云平台服务报告，包括资源消费分析、故障分析复盘、需求问题进展、工单事件分析、监控巡检情况、安全防护分析等；

提供云平台培训服务，包括提供赋能培训和认证考试服务，协助客户熟悉和掌握运营、运维平台功能和自服务使用，同时协助客户打造和管理标准化运维体系、专业化运维团队；

数据中台、应用中台的维护，提供平台产品软件许可更新和技术支持，主要修复软件产品问题，为客户提供软件版本的更新。具体如下：

序号	服务内容	服务描述
1	维护性修复	对产品缺陷提供诊断服务，提供修复或临时解决方案(远程)；对于严重问题修复，提供补丁修复支持服务。
2	软件版本更新	在软件许可更新和技术支持期内，如遇软件版本更新，授权许可甲方使用软件的更新版本。向客户提供软件版本更新许可，主要包含软件补丁、软件新特性和升级版本。
3	远程技术支持	用户在软件产品使用过程中遇到的问题 5*8 的驻场技术支持和 7*24 小时工单、热线电话的远程技术支持

运维服务基础包是以自然年为单位，为客户提供合同范围内的平台运维服务，服务包括项目接口人、服务报告、深度巡检、障处理等基础性运维内容。

序号	服务内容	服务描述	交付件
1	运维服务接口人	客户提供运维服务阶段技术问题的沟通、协调与管理工作，作为数据中台运维服务的接口人。	紧急联系电话
2	年度运维服务报告	每年度提供客户运维服务报告，对运维服务进行总结。	《年度服务报告》

3	重大故障处理	重大故障的应急、推动和处理。	《故障处理报告》
4	平台运维策略制定	运维初期，协助客户制定平台运维策略，规范不同系统、不同等级故障的运维策略、变更时间窗选择原则、所需资源等。	《云平台运维策略建设指导书》
5	深度巡检	平台深度巡检服务。	《平台巡检报告》
6	变更支持	变更方案的审核，并提供技术支持。	《变更方案》
7	小版本升级	不跨版本的小版本升级服务，因客户需求变更的升级。	《升级实施方案》

预防性运维：根据客户需求及现场实际情况编制应急预案，每年定期进行应急演练，用以验证应急预案的可行性。在故障处理方面，联通会严格遵守客户要求的时限进行操作，按时修复，按时上报，并在规定时间内形成书面报告。

用户使用培训：根据云计算技术的发展动态，结合联通多年来的云计算和系统集成培训经验，在广泛听取客户意见、了解客户需求的基础上，联通为该项目特别设计了一套贴近符合项目构建项目所涉及的系统构成，又具有技术前瞻性和先进性的定制培训安排和课程体系，本次的培训对象分为领导层人员、专业技术人员、一般业务人员，针对不同的培训对象设置不同的培训目标和培训重点。

产品（软件）的安装服务、调试调优和补丁修复、版本升级、优化完善：服务期内对 API、容器、微服务、应用系统等产品（软件）提供提供新版本及补丁技术服务。

紧急恢复服务：制定与本项目服务内容相适应的应急预案。根据故障级别启动应急预案，提供应急响应服务，进行故障诊断和系统恢复。应急事件结束后，由应急小组组织应急事件相关人员参与，召开应急事件总结会，对应急事件的故障原因和处理过程进行分析，完善日常预警机制的和应急预案。每年定期进行应急演练，用以验证应急预案的可行性。在故障处理方面，联通会严格遵守客户要求的时限进行操作，按时修复，按时上报，并在规定时间内形成书面报告。

巡检服务：定期提供健康巡检服务。即时检查、发现硬件和系统软件故障隐患，

即时排除故障，不得因硬件和系统软件故障造成业务中断，保持业务持续运行。联通会为客户提供高质量的设备维保服务，核心关键设备会采购原厂维保。同时，联通拥有全 IT 线大量的备品备件，可以最大限度地保障客户硬件维修。联通承诺提供服务响应 7*24 小时电话服务，保证所有信息第一时间接收并反馈。

技术答疑：负责 7*24 小时维护服务电话的接听、维护信息的收集、响应，确保客户需求第一时间得到反馈，为客户提供完整的工单处理流程，保证所有问题快速响应和处理并形成闭环。

数据采集分析报送：本措施以提供周期性的巡检报告为主要内容，对运行服务的服务内容和服务方法进行服务监督，对该项目的服务监控、服务优化、服务配置和安全保障等方面进行运行管理，确保为用户提供安全可靠的主动运行保障服务。每日对系统进行至少一次常规巡检，每月末或月初至少进行一次月巡检，并出具巡检报告，保证系统正常运行。

日巡检报告应包括如下内容：

数据库、主机、存储、中间件(tuxedo，weblogic、Apache)、网络联通性、后台进程的运行情况。

应用软件运行情况，包括各子站流量统计。

系统平台负荷情况。

历史数据是否进行备份

月巡检报告还应包括如下内容：

系统内部数据整理情况。

当月应用软件故障情况。

当月应用软件优化情况。

当月新业务上线情况。

上期存在问题解决情况。

现存在的问题及建议。

系统数据库空间耗用趋势分析。

1.2、 5G专网运维服务

1.2.1、 专业维护体系

中国联通作为历史悠久、实力强大的通信运营商，多年来建立了一套完善的维护

体系，积累了丰富的运行维护经验，培养了众多精通技术、训练有素、认真负责的高素质的维护人才，打造了完善的网络性能监控体系。

为了满足客户需求，使客户获得更加及时的服务，中国联通的VIP客户响应中心，由最富有经验的网络运维人员组成，专门负责为重要的VIP用户提供最高品质的维护和服务，保证客户网络7*24小时的运行可靠性和安全性。VIP客户响应中心的服务范围包括一点受理客户申告、主动式故障处理进度的反馈、故障处理结果的证实、事后故障分析报告的提供以及业务技术咨询等。

中国联通设立有统一的VIP政企客户服务响应号码10019，一旦有VIP客户向我们的服务热线提出了故障申报，值班网管人员将立即在网管上直接处理，并可以调动公司的其它相关网络维护部门，以在最短的时间内完成故障处理、恢复电路的工作。中国联通通过高效、简化的故障处理闭环工作流程和电子化故障处理指挥系统，建立VIP政企客户故障处理的绿色通道，使政企客户的故障受理、确认、定位及故障修复时间大大缩短，有效保障客户网络畅通。

为提高业务响应速度，完善组织机构，责任落实到位，使支撑工作、业务响应能力满足市场激烈竞争的需要，向客户提供高运行质量的网络服务，为用户提供网络优化咨询等增值服务，满足客户的一些个性化网络服务需求，中国联通还建立了独特的集团、省、本地网三级业务响应体系。

1）中国联通的三级业务响应体系的工作目标是：

建立“一个体系”，提供“两种服务”，满足“三个需要”，实现：“四个转变”。即建立集团、省、地市三级业务相应体系；提供前台网络支撑服务、客户差异化网络服务两种服务；满足市场竞争、客户需要、企业发展三个需要；实现由被动的网络维护向主动的网络服务转变、由唯一的差异化服务向多样化的差异化网络服务转变、从关注局端运行质量到关注全程端到端运行质量转变、由粗放型网络服务到专业细分转变的四个转变。

2）中国联通集团的三级业务响应体系的特点是：

- 提供一点受理，全面服务。
- 专业技术人员受理，及时准确进行故障定位、指挥、调度、监控故障处理，建立政企客户故障处理，建立政企客户故障处理绿色通道。
- 政企客户服务经理制，为政企客户提供个性化，面对面的服务。
- 提高客户服务满意度。

中国联通建立的集团、省、本地网三级业务响应体系，是以落实业务响应责任和提高业务响应能力为原则，在集团网管中心与省、本地网建立三级业务响应机构，承担对市场经营部门进行后台支持和对政企客户全程、全方位网络服务的职责，具体包括：

(1) 组织协调后台部门对政企客户和市场部门的业务开通和故障处理，及时反馈业务开通信息、提供开通测试报告等；

(2) 规范和考核电路开通及时率、故障处理及时率等工作，制定并执行SLA规范，对政企客户推行差异化网络服务，及时提交故障处理报告和网络运行报告等；

(3) 依据网络能力进行新产品加工整合工作，最大限度的发挥网络的经济效益；

(4) 编制产品目录和使用说明书并定期更新，为市场部门提供支撑。

凭借三级响应体系，中国联通将为政企客户提供“零延时客户服务响应”，严格执行“就近申告”和“一点申告”的客户响应管理规定，中国联通在收到用户故障申告后第一时间进行故障的处理。

除此之外，中国联通还继续加强了对政企客户提供的标准网络服务，如及时开通业务并按要求提供开通报告、及时处理故障并按要求提供故障报告等，同时要进一步提供差异化的网络服务，如客户网管、提供运行报告、按客户级别定义的网络服务标准、甚至客户自定义的相关服务。

中国联通以政企客户需求为导向，以快速响应为手段，还建立了具有市场竞争力和企业特色的差异化网络服务体系。为保障业务响应工作的顺利开展，业务响应部门还配备了相当数量的经验丰富的专业技术和维护人员，为政企客户提供交换、传输、数据、移动以及接入终端的技术支持，组织和实施网络服务，并提供综合解决方案。

以中国联通北京分公司为例，北京分公司 VIP 客户响应中心成立于 2003 年 7 月 1 日。它以提供全面、高效的政企客户服务为己任，依托北京分公司先进的网络技术、强大的网络运维能力和丰富的网络管理经验，构建专业化通信保障平台。提供 7×24 小时全称不间断的服务，专业技术人员实时在线支持；综合考虑长途、本地和接入段的故障，保障障碍修复时间；根据客户要求的时限，及时开通电路；专线电路的传输质量指标、电路可用率高于行业标准。

中国联通通过完整的、快速反应的组织架构，有效地调度集团的网络资源，加强服务质量各环节的受控管理，保障对政企客户服务绿色通道的后台支撑，使整条服务链形成一个有效的闭环流程，为客户 5G 专网项目提供最良好的全程技术服务支持保障。依托于中国联通强大的网络资源优势，经验丰富的运营维护队伍，中国联通将为客户 5G 专网建设提供全面的服务保障与支持。

此外，中国联通不仅可以做到网络层面的客户响应，而且还可以做到业务层面的客户响应。中国联通根据客户的特殊需求，可以制定个性化通信解决方案，满足多样性的差异化服务。

本项目为设备服务租用性质，宏基站、室内分布式皮基站的设备维护工作由运营商负责，部署于机房的边缘计算设备由运营商和客户企业管理部共同维护。

1.2.1.1、 割接处理服务

中国联通对涉及客户 5G 专网业务的割接工作，提前 5 天通知客户，取得客户同意后才可实施，且割接时间安排在周末 0:00~6:00，尽量做到不停或少停业务。设备变更的时间，需与客户书面沟通确定，尽量减少对客户工作的影响，不论工作时间还是非工作时间，承诺都不另行收费。

1.2.1.2、 重大时刻通信保障值守服务

中国联通拥有百年历史，建国以来承担了党和政府历年来所有重大通信保障活动，在大型活动的网络规划、业务提供、指挥调度、项目管理、服务保障和应急保障等方面积累了丰富的经验。

中国联通员工用行动践行了严谨、专注、敬业、坚守的匠心精神，以高度的责任感和使命感，不仅在重大国际国内政治和体育事件中承当重大重保活动，比如，新中国成立 60 周年庆祝活动、新中国成立 70 周年庆祝活动、抗日战争胜利 70 周年庆祝活动、建党 90 周年大庆、党的十九大、历年两会、APEC 会议、一带一路高峰论坛、中非论坛、北京奥运会、世界田径锦标赛、北京冬奥会……，也常年承担了政府和企业重要事件或业务高峰的重保活动，如全国中农工建交邮 6 大国有顶级银行、交招中信广发光大等等其他各大全国性重要银行和银保监会每年金融年终结算，以及淘宝、天猫、京东等等互联网电商巨头的双 11，618 等引发各种全国网民消费热潮购物节，春运期间的中国铁路客运票务网络 12306 等等。在网络洪峰和可靠性的双重压力之下，联通网络安如磐石，守护客户业务安全度

过各种重大考验。联通通信重保服务的金字招牌在历年的政企业务重保的磨砺下日益闪光。

中国联通将在重大事件及会议期间、割接后或其它可能对业务产生重大影响的时刻，为客户提供全程人员现场值守、电话支持等形式的重保服务。

中国联通可以为客户提供不同级别的重保，包括重点监控、保障公示、线路巡检、事前测试、网络操作规避、优先故障处理、故障处理报告、重保记录报告、重保应急预案等项目服务（根据重保级别不同，相应服务内容有所不同）。客户只需要根据自身需求，提出即可。中国联通就会按照重要通信保障服务原则为客户提供最优质的服务：

统一领导、分级负责原则

集团设置总体指挥小组，根据事件响应级别，由项目经理对项目的重要保障的各项工作统一指挥。

快速反应原则

建立重要保障的快速反应机制，在确保一定的人力、物力、财力的储备的基础上，确保在发现、报告、指挥、处置等各项环节的快速反应和紧密衔接。

常备不懈原则

重要保障相关部门要对突发事件有应急预案方面的准备和思想上准备，抓好应急通信保障的演练工作，做到常备不懈，平战结合。在保障过程中，要合理调整设备配备，充分利用现有资源。

网络能力最大化原则

在网络资源向需要优先保障重点区域的同时，要最大限度地发挥网络能力，为客户提供服务。

1.3、 故障处置与报告

故障处置与报告采用分级响应机制，根据故障影响程度划分为三级：一般故障响应时限≤2 小时，严重故障≤30 分钟，灾难性故障需立即启动最高响应。处置流程包含五个核心环节：故障确认阶段通过监控工具实时收集异常指标及日志，规定时间内完成初步影响范围评估；应急处理阶段优先启用冗余资源保障核心业务连续性，对中毒服务器实施网络隔离，同时备份当前数据状态防止覆盖；根因定位阶段结合网络探针、日志聚类工具进行端到端诊断，重大故障由应急小组会商

确定故障源；修复验证阶段在沙箱环境测试补丁或配置变更，通过自动化脚本验证功能恢复后部署生产环境，业务部门同步进行业务流验证；报告闭环阶段 72 小时内出具技术分析报告，包含时间线、根因、处置措施及改进计划，普通故障报告 2 小时内提交，重大故障报告需附加根因分析及预防策略并 24 小时内完成。全过程遵循"数据保全优先"原则，医疗场景严格执行数据本地化加密传输与备份验证，确保符合"数据不出院"要求。所有操作记录通过统一运维中台留痕，支持操作溯源与合规审计，季度故障分析会议输出优化措施并迭代预案，最终提升普通故障修复成功率、系统可用性等。

2、 应急处理措施

2.1、 应急响应方案适用范围

本预案适用于 5G 边缘云平台故障，主要用于通信事故、自然灾害（洪水、地震、台风、泥石流等）、反恐事件、公共突发事件（如“非典”、禽流感疫情等）、重要通信保障任务、法定节假日、重大活动（国事会议、大型体育运动会等）、军事演习等应急通信保障。

2.2、 应急处理的目标及原则

本项目我公司的应急处理目标为“零故障、零中断、零投诉”，遵循“快速响应、业务优先、数据安全、协同配合、持续改进”的原则。

以方法论、实践论、经验库以及体系手册为指导，着重于各运维专业联动保障的全流程管控，切实做到“四到位”：思想认识到位、组织保证到位、处置措施到位、保障人员到位，真正做到计划周密、部署有方、沟通顺畅、权责明确、执行严格、管控有力的“六要素”。

应急保障前组织备件现场存放情况的检查，确保易损备件确实就近存放。核实保障期间的备件配备实际情况，条件具备时组织实战演练。

云平台维护单位应加强应急预案的培训教育工作，定期与不定期相结合地对有关应急处置组织和系统保障人员进行培训。定期培训是指每年至少组织一次，可结合应急预案的推演或演练进行。不定期培训是指系统上线、应急预案变更等情况下必须组织的培训。

明确事件的应急指挥决策机制，负责事件的预防预警、应急处置、报告和调查处理工作，应急管理应遵循“谁主管谁负责、谁运行谁负责”、“统一指挥、密切

协同；注重预防、减少风险；科学处置、及时报告；以人为本、公平优先”的原则。

2.2.1、 应急响应体系设计

为有针对性的做好支持该项目的网络与信息系统安全的应急保障工作，提高5G边缘云的网络与信息系统安全应急保障能力和水平，根据5G边缘云的应急工作特点，我公司结合公司自身应急管理规定与5G边缘云的实际情况进行制定5G边缘云的综合应急预案，包括机房、云平台、网络、安全、迁移、运维等方面的突发事件的应急处置路径。

2.2.2、 应急响应体系建设

2.2.2.1、 应急响应预案编制目的

我公司为该项目建立一个健全的网络与信息系统安全的应急工作保障机制，预防和减少数据中心、云平台、内外部网络与信息系统安全事件带来的损失与危害，保障5G边缘云的稳定运行。

2.2.2.2、 应急响应标准依据

应急预案的编制以国家和江西省相关法律法规为标准和依据，满足各项法律法规的要求，包括：

《中华人民共和国网络安全法》

“第五十三条国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对安全事件进行分级，并规定相应的应急处置措施。”

2.2.2.3、 应急响应工作原则

应急响应必须充分发挥该项目相关各方力量，共同做好5G边缘云应急保障工作。应急响应必须遵守以下原则：

1）预防为主，预防与应急相结合，建立重大故障的预案制度。完善重大故障监控和管理机制，积极采取有针对性的应急准备，防备重大事件的恶化。

2）分级处置，明确重大事件的等级范围、划分依据，制定相应的应急响应流程，先重点后一般，先抢通后修复，最短时间恢复业务。

3）明确应急响应工作的组织机构，保证各项工作责任到人，应急响应领导小组统一负责重大应急事件的组织和指挥工作。

4）统一指挥、密切协作、快速反应、精准执行、科学处置，相互配合，进行业务恢复和故障处理工作，并进行全程跟踪。

2.2.2.4、 应急方案完善机制

根据数据中心、云平台、网络以及安全攻防应急演练等模拟场景总结分析得出的不足和薄弱环节以及提出的改进措施，我公司定期对应急方案进行全面修订与完善。在应急方案中明确更新后的技术架构与系统配置要求、优化后的应急响应流程与信息通报机制、改进后的人员组织架构与职责分工、以及强化后的培训与演练计划等内容。同时，对应急方案的版本管理与更新机制进行规范，确保应急方案能够及时适应 5G 边缘云技术发展、业务变化以及外部环境的动态变化需求，始终保持其有效性与实用性。

通过以上中后期总结与改进措施的实施，5G 边缘云能够不断优化其应急响应机制，提高应对突发事件的能力与水平，为云数据中心的稳定运行与业务持续发展提供坚实可靠的保障。

2.2.3、 应急保障组织

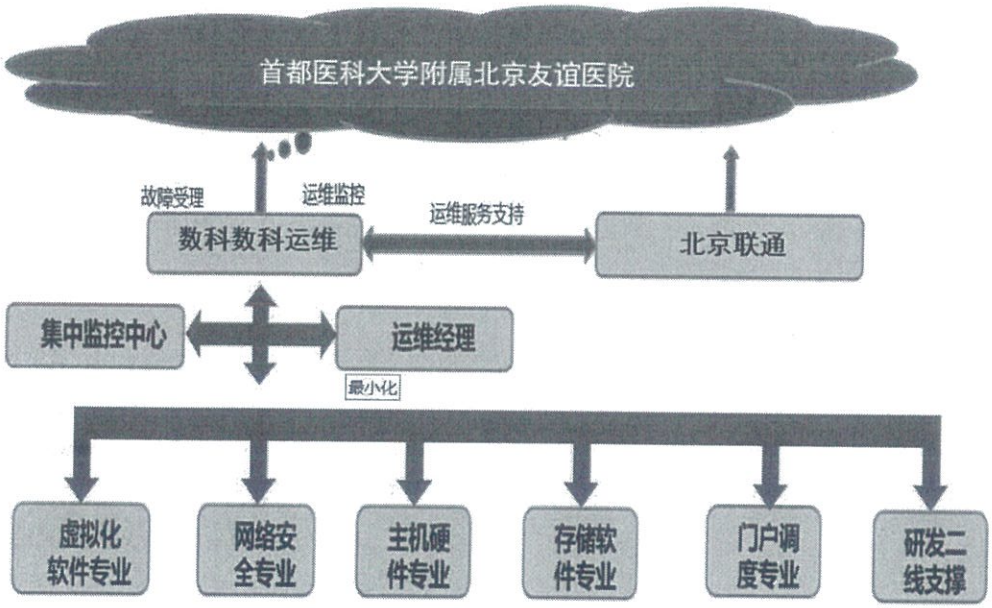
5G 边缘云承载医疗机构的业务系统，数据中心的安全防护至关重要，数据中心的安全防护面扩大，云平台及医疗应用业务面临着来自多方面的潜在威胁，包括自然灾害、电力故障、网络攻击、设备故障以及人为失误等，这些风险因素一旦触发，极有可能导致数据丢失、业务中断，进而引发严重的经济损失、声誉损害以及社会影响。

为了有效应对这些可能出现的突发状况，确保云数据中心在紧急情况下能够迅速、有序地开展应急响应与恢复工作，建立一套完善且高效的应急组织机构与人员方案势在必行。此方案旨在明确在应急事件发生时，各个相关部门、岗位及人员的职责分工、协作流程以及行动准则，通过合理的组织架构搭建和人员配置，最大程度地提高应急处置的效率与质量，降低突发事件所带来的负面影响，保障云数据中心的持续稳定运行以及其所支撑业务的连续性，为 5G 边缘云的数据安全与业务发展筑牢坚实的应急保障防线。

2.2.3.1、 应急保障目标

在数字化医疗快速发展的当下，为全力保障该项目的稳定运行与高效服务，切实达成应急保障目标，全方位做好云计算平台应急服务支撑工作，组建专项应急保障团队架构。成立应急服务领导小组，负责整体应急策略的规划与决策，协调各方资源，确保应急工作的高效推进与精准实施。同时，设立专业应急服务工作小组，这些专业人员将凭借其精湛的技术能力和丰富的实践经验，针对该建设项目可能面临的各类突发状况，如系统故障、网络波动、数据安全威胁等，制定详细且切实可行的应急预案。在应急事件发生时，能够迅速响应，第一时间进行故障排查与诊断，精准定位问题根源，并及时采取有效的修复措施，确保云资源池的持续稳定运行，为医院的医疗业务正常开展提供坚实可靠的技术保障，助力医院数字化建设稳步前行，提升医疗服务质量与效率，守护广大患者的健康权益。

2.2.3.2、 应急保障组织图



2.2.3.3、 应急保障领导组

负责根据 5G 边缘云的应急保障服务的要求，统一指挥、协调部署、组织监督、督导检查应急保障工作的执行。

2.2.3.4、 应急保障组

职责：负责根据领导小组的要求，做好 5G 边缘云中云主机与存储系统，底层虚拟化和分布式存储，云管平台，各类软件故障和隐患，网络系统应急保障，以及平台的底层重大疑难事件应急保障升级处置工作，应急保障期间快速受理及时处

置客户申报的各类技术支持和故障事件。

内容：应急保障期间负责提供 7x24 小时监控值班；完成云计算平台监控项的梳理、配置、调优等工作；

紧急处置快速恢复应急保障期间 5G 边缘云出现的各类门户故障和隐患。检查云平台门户无法使用既无法创建资源、公网 IP 网络或端口不通、云主机关机、开机或重启失败等开通问题，并对隐患进行修复。

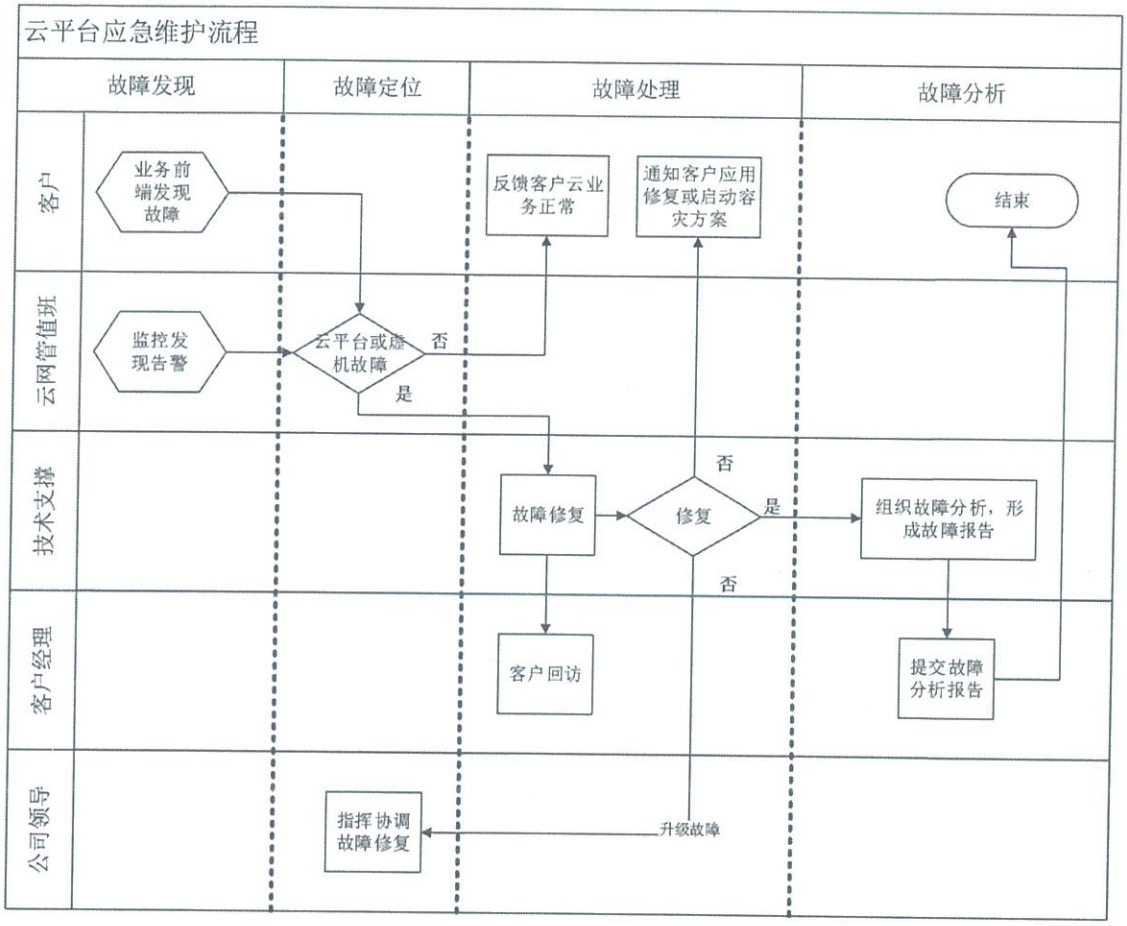
紧急处置快速恢复应急保障期间出现的各类网络故障及隐患。应急处置资源池失联-资源池外部及内部故障事件，以及网络不稳定-资源池外部及内部故障事件等。

2.2.3.5、 应急响应流程、分级机制

应急响应流程犹如一幅精密的导航图，在遭遇危机突发之际，为 5G 边缘云的运维、应急团队及相关业务方指引方向，明确各个环节、各个岗位应当采取的应急行动步骤与协作方式，确保云平台的应急处置工作能够有条不紊地展开。而分级机制则恰似一把精准的标尺，依据突发事件的性质、规模、影响范围以及危害程度等多维度因素，将其划分为不同的等级，如一般事件、较大事件、重大事件和特大事件等，针对不同的等级制定相应的响应策略、资源调配方案以及沟通协调机制，从而实现应急资源的优化配置与高效利用，避免因过度反应或反应不足而导致的资源浪费或应急延误。通过科学合理的应急响应流程与分级机制的构建与实施，云数据中心能够在面对紧急情况时，迅速调动一切可用资源，最大程度地降低损失，保障数据的安全与业务的连续性。

2.2.3.5.1、 应急响应流程

遵循快速响应原则，要求应急人员接到突发事件报告（运维人员巡检异常预警反馈或者接到业务侧故障排查请求）后，应在 15 分钟内启动应急响应机制，并在 2 小时内完成初步处置，输出初步应急报告。整体应急响应流程如下：



（1）事件监测与发现：通过数据中心的监控系统（包括硬件监控、软件监控、网络流量监控、安全监控等）实时监测各类异常情况，如设备故障报警、性能指标异常波动、安全事件告警等。一旦发现异常，立即启动事件报告流程。

（2）事件报告与评估：相关人员在发现异常后，按照规定的渠道和格式向应急指挥小组报告事件详情。应急指挥小组迅速组织技术人员和专家对事件进行初步评估，确定事件的性质、影响范围、严重程度等关键因素，以便确定应急响应的级别。

（3）应急响应启动：根据评估结果，启动相应级别的应急响应预案。不同级别对应不同的资源调配和处理措施。例如，低级别的事件只需要局部技术团队进行处理，而高级别事件需要全员参与，甚至协调外部资源。

（4）应急处理实施：各应急小组按照预案分工开展工作。技术支持小组进行故障修复或系统调整，安全应急小组加强安全防护，业务协调小组与业务部门沟通并协助业务恢复，后勤保障小组保障物资供应。在处理过程中，要保持信息的及时传递和共享，应急指挥小组实时掌握处理进度并进行协调指挥。

（5）事件恢复验证：在采取应急处理措施后，对数据中心的各项服务和系统进

行全面测试和验证，确保故障已排除，系统恢复正常运行，业务数据完整且可正常使用。验证通过后，逐步恢复业务服务，并继续进行一段时间的监控观察，确保问题不再复发。

（6）应急结束与总结：当云数据中心各方业务恢复正常运行且稳定一段时间后，宣布应急处理结束。之后组织全面的总结会议，对应急事件的处理过程进行复盘，分析事件原因，评估应急处理效果，总结经验教训，对应急预案进行修订和完善，以提高未来应对类似事件的能力。

2.2.3.5.2、 应急响应分级机制

5G 边缘云上承载的业务种类繁多，根据影响程度进行应急响应分级处置，响应机制如下：

一般故障（一级响应）：对 5G 边缘云整体运行影响较小，仅涉及个别设备或系统的局部故障，如单台服务器硬件故障、部分网络链路波动等。此类事件可由技术支持小组在较短时间内独立解决，对业务的影响轻微或可通过冗余机制自动切换而基本无影响。

严重故障（二级响应）：影响到 5G 边缘云上部分重要业务服务或多个业务系统的故障，如医院业务区域的服务器集群故障、核心网络设备的部分功能故障等。需要技术支持小组、安全应急小组和业务协调小组协同处理，可能需要调配一定的备用资源，处理时间一般在数小时内，我公司应急人员与客户业务部门可能需要采取一些临时应急措施，如部分业务功能受限或延迟服务。

紧急故障（三级响应）：严重影响 5G 边缘云整体运行，导致大量业务中断或数据面临严重安全威胁，如数据中心电力系统故障、大规模网络攻击导致数据安全问题、核心存储系统故障等。此时启动全面应急响应，应急指挥小组统一调度所有应急小组，全力投入应急处理，可能需要协调外部供应商提供紧急技术支持和资源，处理时间可能较长，需联合业务部门制定业务切换到备用数据中心或其他临时替代方案的计划，以减少长期业务损失。

重大故障（四级响应）：极端情况下，如自然灾害（地震、洪水等）导致云数据中心基础设施严重损毁，数据中心面临长时间甚至永久性瘫痪的风险。这需要最高级别的应急响应，除了内部应急组织全力应对外，还需要与政府相关部门、行业组织等外部机构密切合作，进行数据中心的紧急抢修或考虑数据迁移到异地备

用数据中心等长期恢复方案，业务恢复时间难以预估，且可能面临巨大的业务变革和数据重构需求。

2.2.3.5.2.1、 应急工作评审

为了做好应急准备工作，我公司每年组织 1 次应急工作评审。这次评审旨在依据审核结果督促我公司完善信息系统，深化应急准备工作，对我公司信息系统和应急准备措施进行全面检查和评估，以确保在应对突发事件和灾害时有足够的准备和有效的应对措施。

在评审过程中，项目负责人、云平台管理方将根据审核结果提供具体的意见和建议，以督促我公司完善信息系统和深化应急准备工作。这些建议可能涉及技术方面的改进、流程的优化以及员工培训等，旨在提高我公司在应急情况下的应变能力和协调能力。

在完善信息系统方面，我公司需要加强对 5G 边缘云涉及的硬件设备和软件程序的维护和更新，以确保系统的稳定运行和安全防护。除此之外我公司还要加强网络和信息安全管理，采取有效的防护措施和应对策略，以应对可能的网络攻击和数据泄露。

深化应急准备工作意味着我公司需要制定完善的应急预案和相应的流程，明确各个岗位的职责和应急响应措施，并进行定期的演练和培训，提高员工应对突发情况的能力。与此同时，我公司还要建立和相关部门、机构的合作关系，建立起紧急联系机制，以便在需要时能够及时协调资源和应对措施。

云管理方的督促和指导对于我公司的应急准备工作至关重要，可以通过定期的进度评估、随机的应急演练和督导检查等方式来督促我公司完善工作。通过这样的方式，云管理方可以及时了解我公司的应急准备情况，发现问题并及时提供支持和帮助，以确保信息系统的安全性和可用性。

2.2.3.5.2.2、 应急事件级别定义

根据网络与信息安全突发公共事件的可控性、严重程度和影响范围，一般分为四级：I 级（重大故障）、II 级（紧急故障）、III 级（严重故障）、IV 级（一般故障）。国家有关法律法规有明确规定的，按国家有关规定执行。

（1）I 级（重大故障）：5G 边缘云上的首都医科大学附属北京友谊医院有业务瘫痪，无法提供服务，如火灾、水灾、电力等导致的数据中心以及数据无法应急使

用。

（2）II 级（紧急故障）：5G 边缘云上的首都医科大学附属北京友谊医院的系统核心业务瘫痪，无法提供服务，如数据库服务器、核心设备、云平台完全瘫痪宕机等。

（3）III 级（严重故障）：5G 边缘云上的首都医科大学附属北京友谊医院的系统核心业务仍能提供服务，但是性能受到严重影响，如网络波动，云平台服务卡顿，数据库响应极为缓慢等。

（4）IV 级（一般故障）：5G 边缘云上的首都医科大学附属北京友谊医院的系统业务不受影响。

2.2.3.6、 应急响应沟通机制

应急响应沟通机制起着传递信息、协调各方行动以及保障整体应急处置工作顺利推进的关键作用。应急响应过程涉及云数据中心内部的多个部门与专业团队，包括运维人员、安全专家、技术支持工程师等，同时也关联着外部的客户，如用户、合作伙伴、上级监管部门以及相关技术服务供应商等。在这样一个多主体、多环节的应急情境下，若缺乏有效的沟通机制，信息的传递将变得迟缓、不准确甚至中断，进而导致应急决策的失误、资源调配的混乱以及救援行动的延误。例如，运维人员若不能及时将故障的详细信息传达给安全专家，可能会延误对网络攻击的有效应对；用户若无法及时获取事件进展与恢复时间的通报，可能会引发恐慌与不满，对用户声誉造成损害；而云数据中心与外部供应商之间若沟通不畅，在急需特定技术资源或设备时则可能无法及时获得支持，从而延长系统恢复的时间。针对于首都医科大学附属北京友谊医院 5G 边缘云项目构建一套健全、高效且适应性强的项目应急响应沟通机制具有极为重要的现实意义。该机制旨在通过明确沟通主体、规范沟通渠道、制定沟通流程与信息模板，确保在应急事件发生的第一时间，准确、及时且完整地传递各类关键信息，实现内部各部门之间的无缝协作、外部利益相关者的充分知情与积极配合。

2.2.3.6.1、 团队间沟通机制

应急指挥小组：负责整体应急响应的决策、指挥和协调工作。评估事件的严重程度，确定应急响应级别，并根据情况启动相应的应急预案。与外部相关机构（如监管部门、合作伙伴等）进行沟通协调，代表数据中心对外发布信息。

技术支持小组：包括网络工程师、系统工程师、数据库管理员等专业技术人员。负责对事件进行技术层面的分析、诊断和处理。恢复受影响的系统、网络和数据，实施技术层面的应急措施，如网络隔离、数据备份恢复、系统修复等。向应急指挥小组及时汇报技术处理进展情况和遇到的问题。

业务运维小组：与数据中心客户保持密切联系，负责及时向客户通报事件情况，解答客户的疑问和关切。收集客户反馈的信息，并传递给应急指挥小组和技术支持小组，以便更好地处理事件和满足客户需求。

安全防护小组：负责应急处置，实时溯源以及向应急指挥小组进行进度汇报，与技术支持小组进行实时沟通，快速定位故障，实时处置。

后勤保障小组：根据应急指挥小组、业务运维小组、安全防护小组等的应急响应要求，实时沟通，实现后勤保障。

2.2.3.6.2、 事件监测与报告流程

事件监测：

建立全方位的监控系统，包括网络监控、系统性能监控、安全监控等。

监控系统实时收集数据中心内各种设备、系统和应用的运行数据，并进行分析。

设定预警阈值，当监控数据超出正常范围或检测到异常行为（如网络攻击、系统故障、数据异常等）时，自动触发警报。

事件报告：

监控系统发现异常后，立即向技术支持小组发送警报通知。

技术支持小组在接到通知后，第一时间对事件进行初步评估，确定事件的性质、影响范围和可能的原因。

2.2.3.6.3、 内部沟通流程

（1）应急指挥小组会议：

在接到事件报告后，应急指挥小组立即召开紧急会议，参会人员包括技术支持小组负责人、业务运维小组负责人、业务运维小组负责人等。

会议上，技术支持小组详细汇报事件的技术细节、进展情况和预计的处理时间。

业务运维小组汇报客户反馈和关切的问题。

应急指挥小组根据各方汇报情况，制定进一步的应急处理策略和沟通计划，明确各小组的下一步工作任务和时间节点。

（2）技术支持小组内部沟通：

技术支持小组内部通过即时通讯工具、电话会议等方式保持实时沟通。

网络工程师、系统工程师、数据库管理员等成员及时共享各自负责领域的技术信息，协同分析事件原因和制定解决方案。

技术支持小组负责人定期（每小时）向应急指挥小组汇报技术处理进展情况，遇到重大问题或需要决策时随时汇报。

（3）跨小组信息共享：

建立专门的应急响应信息共享平台，各小组将相关信息（如事件报告、处理进展、客户反馈、舆情信息等）及时上传到平台。

各小组成员可以随时访问平台获取所需信息，确保整个应急响应团队对事件的整体情况有全面、准确的了解。

定期（每 2 小时）召开跨小组沟通会议，各小组汇报工作进展，协调解决存在的问题，确保应急响应工作的协同推进。

2.2.3.6.4、 外部沟通流程

（1）客户沟通：

业务运维小组通过电子邮件、短信、电话等多种方式与客户保持密切沟通。

在事件发生后的 1 小时内，向所有客户发送详细的事件通报邮件，包括事件发生时间、影响范围、目前的处理进展和预计恢复时间等信息。

每 2-4 小时向客户更新一次事件处理进展情况，直至事件完全解决。

设立专门的客户咨询热线和在线客服，及时解答客户的疑问和处理客户的投诉。

在事件解决后，向客户发送事件总结报告，说明事件原因、处理过程和预防措施，以增强客户对数据中心的信任。

（2）合作伙伴沟通：

应急指挥小组或指定的联络人负责与数据中心的合作伙伴（如供应商、合作运营商等）进行沟通。

在事件发生后，及时通知合作伙伴事件情况，特别是可能影响到合作伙伴业务或合作关系的情况。

与合作伙伴共同评估事件对双方合作的影响，协调资源共享和技术支持，共同应对事件。

在事件处理过程中，定期向合作伙伴通报进展情况，在事件解决后，与合作伙伴总结经验教训，完善合作应急机制。

（3）监管部门沟通：

业务运维小组协同应急指挥小组，按照相关法律法规和监管要求，及时向监管部门报告事件情况。

报告内容包括事件的详细经过、影响范围、采取的应急措施、预计的恢复时间等。

在事件处理过程中，积极配合监管部门的调查和监督，及时回复监管部门的询问和要求，提供相关的资料和信息。

在事件解决后，向监管部门提交详细的事件处理报告和整改措施，确保数据中心符合监管要求。

2.2.3.6.5、 沟通文档管理

（1）事件记录文档：

由技术支持小组负责创建和维护事件记录文档，详细记录事件的全过程，包括事件发生时间、发现过程、初步评估、技术分析、处理措施、恢复过程等信息。

事件记录文档应实时更新，确保信息的准确性和完整性。

在事件解决后，将事件记录文档进行归档保存，以便后续的分析总结和审计。

（2）沟通记录文档：

各小组在与内部成员、客户、合作伙伴、监管部门和媒体等进行沟通时，应详细记录沟通的内容、时间、对象等信息。

沟通记录文档由各小组自行管理，并定期（每天）汇总到应急响应信息共享平台。

应急指挥小组可以随时查阅沟通记录文档，以便全面了解应急响应过程中的沟通情况，及时发现问题并调整沟通策略。

（3）信息发布文档：

业务运维小组负责整理和保存所有对外发布的信息文档，包括新闻稿、声明、客户通报邮件、社交媒体发布内容等。

信息发布文档应经过审核和批准流程，确保信息的一致性和合规性。

在事件结束后，对信息发布文档进行评估和总结，分析信息发布的效果和存在的问题，为今后的应急响应沟通提供经验参考。

2.2.3.6.6、 沟通培训与演练

（1）沟通培训：

定期（每季度）对各应急响应小组成员进行沟通培训，提高成员的沟通能力和技巧。

培训内容包括应急响应流程中的沟通规范、与不同对象（客户、媒体、监管部门等）沟通的要点和方法、信息传递的准确性和及时性要求等。

邀请专业的沟通专家进行授课和案例分析，通过模拟演练等方式让成员在实践中掌握沟通技能。

（2）应急演练：

进行应急演练，按照院方要求，进行系统故障演练，包括事件模拟、应急响应流程执行和沟通机制的检验。

在演练过程中，重点关注各小组之间的沟通协作是否顺畅，信息传递是否及时准确，对外沟通是否有效等方面。

演练结束后，对沟通环节进行详细的评估和总结，针对存在的问题制定改进措施，并对应急沟通机制进行优化和完善。

通过建立这样一个完整的云数据中心应急响应沟通机制，可以确保在面对突发事件时，数据中心能够快速、有效地进行内部协调和外部沟通，最大限度地减少事件的影响，保障 5G 边缘云的稳定运行和客户的利益。

附件四《中标通知书》

中技国际招标有限公司

CHINA INTERNATIONAL TENDERING LIMITED COMPANY

编号 Ref. No.: ITCYW-6

日期 Date: 2025年9月11日

发件人 From: 马建

致：联通数字科技有限公司

北京友谊医院顺义院区应用系统与研究所信息化建设项目（医院部分）招标

（招标编号：0701-254106140767）

中标通知书

关于标题项目，经评标委员会评审，并经采购人审批同意，兹通知贵单位在如下内容的招标采购中中标：

包号	品目号	标的名称	数量	中标金额（人民币元）
1	1-1	5G边缘云管理平台	1项	1,298,860.00

请贵单位于本通知书发出后3日内与采购人联系，在本通知发出后30日内签署采购合同，采购合同签署后将合同扫描件发送至邮箱：majian4@cgci.gt.cn，我司将在收到合同扫描件后5个工作日内将投标保证金原路退回。

采购单位：首都医科大学附属北京友谊医院

采购人联系电话：010—63138216

我公司地址：北京市丰台区西营街1号院通用时代中心C座9层

联系人：马建　　联系电话：81168697

谢谢参与！

中技国际招标有限公司

2025年9月11日

抄送：首都医科大学附属北京友谊医院