合同编号：JSCZE2104901CGN00

合同文本：

常州市金坛区卫健信息化平台
“5G+云计算”服务业务合作协议

甲方：常州市金坛区卫生健康局
法定代表人：袁永炜

乙方：中国电信股份有限公司常州分公司
法定代表人：黄亚君

为全面加快医疗信息化发展步伐，提高卫生信息化建设与应用水平，支撑和保障金坛区域内医疗系统的正常运营，加快发展“5G+云计算”的信息化建设，常州市金坛区卫生健康局与中国电信股份有限公司常州分公司本着“平等友好、互惠互利、合作共赢”的原则，经双方友好协商，就建设“5G+云计算”达成共识，特签订本合作协议。

一、 合作内容

1、5G网络试点建设

甲方将乙方的5G建设作为医疗信息化建设的重点项目，在基站建设、用电、应用推动等方面给予积极协调，全力支持5G试点建设工程。

乙方积极开展应用试点创新，将甲方5G应用与公用5G网络进行隔离，提供私有网络保障，确保甲方医疗数据安全。

2、医疗云服务

乙方发挥自身云资源优势，通过构建“私有云+行业云”的混合云平台，为甲方提供性能成熟、产品丰富的专属医疗云服务。乙方通过“本地存储+存储网关+云存储”的方式，实现医疗数据的便捷、可靠存储；通过备份中心，提升生产业务的高可用性；提供按需使用、快速开通、弹性扩容的各类云产品，满足应用创新、助力互联网医院的建设。

通过发挥甲乙双方各自的资源优势，合作建设扩展能力强、服务范围广、拓展空间大、运营安全稳定性好，打造灵活、智能、协同的专业级区域信息化平台，促进医疗向“云端”的聚集。

乙方承诺提供资源配置：Vcpu500核，内1600G，存储（SAS）56000GB，满足金坛区卫生健康局未来5年业务发展需求。

3、基础通信业务

乙方为甲方提供两条千兆电路，实现内网“云上云下”主备互通。乙方在IDC机房提供机柜供甲方使用。同时乙方需提供备用医保专线，实现医保业务主

备线路保障。乙方保证组建并提供服务的数据中心网络，符合并能够达到信息系统等级保护三级的标准和要求（应该根据甲方需要提供信息系统等级保护测评三级的测评报告，甲方承担信息系统测评费）。

4、维护服务

乙方指定专人对本合同中提供的服务进行 7*24 小时维护（响应时间在 30 分钟内），包括云主机、金坛卫生区域网络、操作系统和数据库，定期向甲方提供安全运维报告。

合同目的必需达到招投标文件约定的实质目的。

二、合作期限及费用

1、本合作协议有效期自[2021]年[7]月[15]日至[2025]年[12]月[31]日。总费用为：￥ 8000000 元，大写：捌佰万元整（增值税税率 6%）。

2、如因特殊情况需提前中止，必须提前[30 日]向对方提出书面申请。经对方同意后方可以终止协议，否则提出终止方应按照本协议第六条之约定承担违约责任。

三、缴费方式

2021 年 8 月 31 日前支付 160 万元；2022 年 8 月 31 日前支付 160 万元；2023 年 8 月 31 日前支付 160 万元；2024 年 8 月 31 日前支付 160 万元；2025 年 8 月 31 日前支付 160 万元。

乙方向甲方提供正规发票后在当月 20 日以前，甲方以转账方式将相应费用缴纳到乙方账户。

2、乙方的银行账号：

开户名称	中国电信股份有限公司常州分公司
开户行	工行金坛支行
帐号	1105027119001113649

四、甲方的权利和义务

1、甲方使用云业务时虚拟服务器内所需的软件和承载的信息等，除合同约定提供的操作系统和数据库软件以外，均由甲方自行提供（包括但不限于域名、网页、程序等）。甲方保证其有权使用/承载该些软件和信息，不会侵犯任何人的合法权益（包括但不限于知识产权、所有权等）。如果有人提出法律或行政程序（合称“侵权指控”），声称甲方侵犯了其知识产权、所有权等合法权益的，甲方应当负责解决，并赔偿乙方就此所承担的一切损失和费用，包括但不限于上述侵权指控中所产生的诉讼费用、合理的律师费用、调查费用、和解金额或生效法律文书中规定的赔偿金额。

2、甲方使用云业务（包括但不限于软件、信息等）必须遵守《中华人民共和国电信条例》、《中华人民共和国计算机信息网络国际联网暂行规定》、《互联网信息服务管理办法》和其他有关法律、法规及相关规定，不得有任何违法违规行为，不得侵犯任何第三方的合法权益。因甲方使用云业务造成的法律纠纷和后果均由甲方自行负责。若因此造成乙方损失的，甲方还应赔偿乙方因此而遭受的损失。

3、甲方不得以任何方式经营未经政府管理部门批准的业务或本协议中未约定开展的业务，包括但不限于：无资质虚拟主机、proxy 代理服务、邮件转发、将互联网带宽以任何方式（包括但不限于私拉光纤进行转接、建立 VPN 隧道等手段）为任何第三方提供穿透流量接入、无资质二次转租等。

4、甲方对其提交的所有信息的真实性、合法性、有效性、完整性负责，并承诺在信息变化时及时通知乙方。

5、甲方应妥善保管和使用自己的业务密码。因使用不当或者被他人盗用（在非乙方原因的情况下）所导致的损失，由甲方自行承担。若系乙方原因，乙方应承担赔偿责任。

五、乙方的权利和义务

1、乙方应保证组建并提供服务的数据中心网络，符合并能够达到信息系统等级保护三级的标准和要求，若因应用软件或业务系统等原因造成无法达到信息系统等级保护三级的标准和要求，由甲方自行负责。乙方应该指导甲方采用配套适合的应用软件或业务系统。

2、乙方提供的主机硬件损坏导致甲方数据泄露、丢失、损坏等的，乙方应承担数据泄露、丢失、损坏后产生的法律、经济等方面的责任。

3、乙方应努力提高服务水平，从技术、日常巡检等方面确保本协议内服务内容运行正常，以确保平台的安全性、稳定性。乙方应全力确保区域信息化云平台的正常运转，并做好应急备份。如出现因乙方的设备等因素而影响正常运行的整个卫生专网故障，必须在 30 分钟内修复，否则即视为一次事故，乙方应出具书面事故报告。

4、为甲方提供大客户级的综合服务，指派专门的客户经理为甲方提供服务，实现 7*24 小时故障受理热线服务，由客户经理作为直接故障和服务受理人员，实现一点负责。

5、乙方出于服务、技术和业务发展的需要，实施线路检修、服务措施更新，以及设备更新和搬迁、工程割接、网络及软件升级等施工建设、技术改造与网络调整，应提前 3 日书面通知甲方，并采取合理可行的应急措施，甲方应当配合。如实施上述项目将影响或者可能影响正常服务，乙方可选择采取电话、广播、电视、公开张贴、报纸或短信、传真、电子邮件、互联网等方式按规定时限提前予

以通告。

6、乙方应为甲方的云业务提供整套安全服务（所提供的安全服务能有效降低黑客入侵之机会，但无法确保杜绝所有恶意行为）。若乙方存在以下情况：1、在没有甲方书面通知的情况下删除甲方的云主机或云储存数据 2、乙方技术人员直接进行数据迁移造成甲方长时间（超过 1 小时）业务无法恢复的，乙方应承担相应的责任并出具书面报告。因不可控不在本业务防护之列的情况包括但不限于：①不能防御已经授权的访问，以及存在于网络内部系统间的攻击。②不能防御合法用户恶意的攻击，以及社交攻击等非预期的威胁。③不能修复脆弱的管理措施和存在问题的安全策略。④不能防御不经过防火墙的攻击和威胁。⑤不能防御合法用户因自身软件缺陷导致的应用攻击。

7、如果因硬件损坏导致数据丢失，乙方应该承担相应的损失。

六、违约责任

任何一方违反本协议规定，均应承担相应的违约责任，违约方应承担因自己的违约行为而给守约方造成的直接经济损失，即一方对另一方因违反本合同而导致的收益或利润损失，未实现预期的节约、商业信誉损失以及数据丢失等其他损失不承担责任。

除本协议另有约定外，若协议任何一方在协议期未满之前单方面提前终止协议或者违反合同约定的，违约方应向守约方支付协议剩余未履行期间月使用费总额作为违约金。

七、不可抗力条款

本协议所称不可抗力、意外事件是指不能预见、不能克服并不能避免且对一方或双方当事人履行本合同造成重大影响的客观事件，包括但不限于自然灾害（包括但不限于洪水、地震、瘟疫流行和风暴等）、社会事件（包括但不限于战争、动乱、恐怖主义、政府管制等）、其他事件（包括但不限于国家法律法规或规章变动、电脑病毒爆发、停电、通信线路被人为破坏等）。

因不可抗力或者意外事件使得本协议的履行不可能、不必要或者无意义的，导致协议双方或一方无法继续履行协议时，受影响方不承担违约责任，但应尽快书面通知对方，并协商适当延长协议的期限。在影响消除后，受影响方应及时通知对方，经协商一致后，本协议继续执行。

因政府管理部门依法要求乙方暂停或终止提供相应服务导致乙方暂停或终止提供本业务的，乙方无需承担任何责任。如乙方已预收甲方业务使用费的，乙方应将甲方未使用部分对应的费用（无息）退还甲方。

八、保密条款

未经对方书面许可，任何一方不得向第三方提供或者披露因本协议的签订和履行而得知的与对方业务有关的资料和信息，但法律另有规定或本协议另有约定

的除外。乙方向其关联公司提供甲方云服务业务有关的资料和信息以及乙方根据相关法律法规及行政主管部门的强制要求提供或披露与甲方业务有关的资料和信息的，不受此限。

九、争议解决方式

所有因本协议引起的或与本协议有关的任何争议将通过双方友好协商解决，如果双方不能通过友好协商解决争议，则提交甲方所在地人民法院裁决。

十、其它

本协议一式肆份，甲乙双方各执贰份。本协议自双方盖章并经乙方授权代表签字后生效，有效期至本协议第二条约定的业务使用期期满之日止。

其他未尽事宜双方另行协商议定或以备忘录、补充协议等形式加以完善。

十一、以下文件是合同不可分割部分：

1、招标文件

2、乙方提供的投标文件

3、中标(成交)通知书

4、合同附件

若本合同及附件与招投标文件有任何冲突，均以招投标文件为准。

附件为本合同不可分割的部分。

本合同附件为：附件一：项目服务清单

附件二：信息安全与保密承诺书

附件三：网络信息安全承诺书

甲方：常州市金坛区卫生健康局

法定或（授权）代表签字：

日期：

盖章：

乙方：中国电信股份有限公司常州分公司

法定或（授权）代表签字：

日期：2021.7.12

盖章：

附件一：项目服务清单

项目服务清单

由于医疗行业系统的特殊性，乙方提供“私有云+行业云”的混合云服务的服务模式，具体服务内容如下：

一、私有云服务

针对 HIS 核心数据库与 PACS 系统：由于该业务对设备性能要求较高，需以“私有云”的方式实现业务稳定运行。

1.1 HIS 系统

HIS 系统采用主备模式建设，单套业务需求如下：

资源配置	cpu（核）	内存（GB）	存储（GB）	存储支持最大读写速度
配置	40	256	8000	2600

1.2 PACS 系统

PACS 业务系统提供主用可用存储空间 20T，备份可用存储 20T，磁盘读写速度 7200 转。

二、行业云服务

乙方提供“行业云”服务，通过“行业云”服务，实现业务的平顺扩展与稳定运行，提供的资源配置如下：

资源配置	Vcpu（核）	内存（GB）	存储（SAS-GB）
配置	500	1600	56000

三、安全服务

乙方提供的整体网络需符合信息系统等级保护三级的标准和要求，实现整体网络安全稳定运行。具体参数如下：

序号	名称	指标项	配置要求	备注
1	云防	基本要	2U 机箱 最大配置为 34 个接口， 默认包括 6 个	需提

	火墙	求和性能	10/100/1000BASE-T 接口、4 个千兆 SFP 插槽、4 个万兆 SFP+插槽和 2 个可插拔的扩展槽和，标配模块化双冗余电源；	供主备各一台，共计两台。
			防火墙吞吐率：40Gbps 并发连接数：800 万	
			含入侵防御功能，服务期内规则库升级许可；	
			含防病毒功能，服务期内规则库升级许可；	
		网络特性	支持路由、透明、混合与虚拟线部署；支持静态路由、PBR 与多播路由，以及 RIPv1/2、OSPF、BGP 等多种动态路由协议；支持 ISL、802.1Q 二层协议封装以及 VLAN-VPN 功能；具有接口联动特性，使同一联动组内所有物理接口的 UP/DOWN 状态同步变化；	
			支持多链路接入环境下的出站多运营商智能选路与入站智能 DNS；	
			支持服务器负载均衡功能，并至少提供 10 种以上服务器负载均衡算法	
		基础安全	能够基于访问控制策略对最大并发连接数限制；支持在 WEB 界面中查看每条策略所匹配的当前会话、历史会话与报文统计信息；具有策略自学习功能，并且能够根据自学习结果直接生成访问控制策略；	
			支持策略冲突检测功能	
			具有防共享接入特性，能够有效识别、报警并阻断局域网网络共享行为	
			至少支持 254 个虚拟防火墙，虚拟防火墙支持 IPv4/IPv6 双栈部署，并能够实现 IPv4/IPv6 双栈的各种安全控制，虚拟防火墙同样支持策略自学习功能；	
		系统安全	支持系统管理员能够通过“用户名＋口令＋图形认证码”方式认证进行登录管理；	

			支持本地多配置文件存储及配置回滚功能，并且可以有选择性的下载“运行配置”、“保存配置”、“备份配置”、配置文件加密下载以及按对象、策略等分类的部分配置文件下载/上传功能；要求具有配置文件自动定时上传到指定外部服务器功能；	
		高级功能	支持传统应用识别，如 QQ、SKY、淘宝、美团、网易邮箱等传统应用的识别和控制	
			内嵌快速扫描、深度扫描双引擎恶意代码防护技术，恶意代码特征库总数大于 700 万，包含蠕虫病毒、后门木马、间谍软件等；能够检测并抵御的攻击至少包括 11 大类，如 IIS webdav、OpenSSL 等拒绝服务类，BSD telnetd、Sendmail 8.12 等溢出攻击类，Pcanywhere12.0、Windows SMB 等网络访问类，漏洞扫描、端口扫描、IP 扫描等扫描类，Gatecrasher、Hack a tack 等木马类，Microsoft Sharepoint2007 Path 等 HTTP 攻击类，Nagios Remote Plug-In Executor 等 RPC 攻击类，Sasser.b、Blaster 等蠕虫类，Microsoft Outlook Web Access 等 WEBCGI 攻击类，Microsoft Windows、NetBIOS 等系统漏洞类，及 Manage Engine Multiple Products File Collector 等其他攻击类型；	
		高可用性	支持主备、负载均衡和连接保护等双机或多机的高可用性部署可实现多心跳接口备份与负载均衡；	
			支持基于接口度量值方式的双机切换条件设置并且通过智能策略联动机制对攻击行为进行动态阻断	
		攻击防护	支持基于接口、应用层协议等流量异常检测功能，能够根据流量阀值、连接数阀值、协议比例异常阀值等条件触发报警规则，并在管理页面上亮起报警灯；	

2	云备份一体机	系统架构	采用 B/S 架构，备份系统服务端软件兼容基于国产操作系统；同时要求基于 WEB 界面的备份与恢复系统软件，系统采用统一平台管理，支持通过同一界面采用授权方式定义灾备能力，至少包括定时备份功能、CDP 实时备份功能、副本数据管理（CDM）功能、容灾接管功能、自动演练功能、自动校验功能、数据库同步复制功能、异地灾备等模授权，以便后期能够灵活的按需扩展，保护成本投入；支持统一的灾备资源管理、灾备域管理、灾备节点管理、节点运行状态管理、作业状态管理、日志报警监控、报表统计等	
		备份存储介质选择模式	支持 D2D2T 方式进行备份集归档，支持接入主流磁带库、VTL，将备份数据通过磁带库进行离线归档保存；支持标准开放磁带格式，可利用第三方工具或自带工具快速从存储介质（磁盘或磁带）中恢复已备份数据。	
			支持 D2D2B 方式进行备份集归档，支持接入主流蓝光存储设备，将备份数据通过蓝光光盘进行离线归档保存。	
			支持备份数据直接写入第三方分布式存储，无需通过备份服务器，提高备份效率，生产数据可直接备份至第三方分布式存储，直接读写数据，性能和速度达到最优。	
			支持将备份数据复制到行业云中，实现云备份异地数据灾备。	
		硬件配置	2U（含导轨），双高速 SSD，12 个 SAS 热插拔盘位，支持 raid1，raid5；标配 1G Cache 阵列卡，可扩展掉电保护；Xeon 双路八核 CPU，64GB DDR4 的 RDIMM 内存，冗余电源，2 个千兆网口，2 个万兆网口；	
			配置功能：可用容量 20T 可用磁盘空间及相应备份授权，含 10TB 实时备份授权，配置无限数量接管授权（最大支持 5 个并发）。	

			软件：64bit 企业级 Linux 内核，基于 WEB 界面的容灾备份系统软件，标配定时备份、实时备份，标配 LAN-FREE 功能等，标配文件/数据库/Windows/Linux/虚拟化定时备份功能，支持 CDP 实时备份，支持自动或一键式容灾接管功能，支持任意时间的接管，支持自动或一键式的仿真演练，支持快速挂载功能。	
		操作系统备份	支持国内主流操作系统的在线热备份保护；要求初始化备份采用完全备份，后期采用差量备份。	
		数据 CDP 实时备份	支持国外或国产环境下数据的 CDP 实时保护功能，满足关键业务系统数据的实时保护；仅单台灾备设备即可实现 CDP 实时保护；不仅可支持单机环境的 CDP 实时保护，还可支持双机环境的 CDP 实时保护；CDP 同步至灾备服务器间隔为≤1 秒，数据挂载与恢复可精确≤1 秒；	
			要求 CDP 实时备份技术采取无缓存备份方式，将数据直接备份至灾备存储介质中，无需在生产机单独提供日志卷作为 CDP 缓存区。	
			恢复支持图形化界面，要求恢复颗粒度可选择（整卷、整盘、分区），支持一键恢复、自定义恢复、在线热恢复、全量+渐进式恢复、只恢复增量数据等多种类型的数据恢复方式，以满足用户不同场景下的恢复需求。	
		数据挂载	支持原机或异机的快速数据挂载功能，可自定义方式输入任意时间点的备份数据进行挂载访问，形成一个临时可读可写的分区，无需进行数据还原过程，从而实现备份数据的可用。	
		数据库备份	支持 Oracle、IBM Domino 邮件数据库、MS SQL、mongo、Postgresql、达梦、人大金仓、南大通用、神通数据库、优炫数据库等国外或国产主流数据库的在线定时和实时备份保护；备份恢复 Oracle 数据库支持自动构建、数据文件重定向、表空间恢复、配置恢复参数文件功能，无需	

			额外改动监听配置即可进行备份保护，支持 Oracle RAC 在线备份保护，支持恢复到单机环境，支持备份集定时自动恢复功能；支持以非脚本的方式对数据库进行保护，支持完全、增量、差量备份。	
			支持 HANA 完全、增量、差量备份。	
		文件保护	支持海量文件备份：支持千万级以上海量文件日志增量备份保护，可快速定位到修改或新增的文件并进行备份，无须每次增量备份时扫描所有文件；增量备份间隔可达分钟级。	
		副本数据管理	支持对核心业务系统 Oracle、Oracle RAC、VMware 等主流应用以原生数据格式进行备份和存储，支持数据恢复无需备份格式转化，支持备份数据即时可用，当业务中断时，可在 5 分钟以内将包括 Oracle RAC 等在内的业务数据即时挂载方式恢复。	
			支持副本数据管理功能，支持备份数据副本分钟级克隆，支持提供同一资源在不同时间点上多个副本的集中管理，副本挂载后生成新的挂载副本，支持同一时间点副本下产生多个挂载副本、支持对生成副本进行读写、支持无需通过任意网络进行数据传输移动的即时恢复特性。	
		虚拟化和云平台数据备份	支持 VMware、华为虚拟化、华三虚拟化、Hyper-V、深信服等虚拟化环境的整机备份与恢复，采取无代理方式备份，支持 Lan-Free、完全备份、增量备份、差异备份、永久增量等备份方式；支持快速定位需要备份的虚拟机，并添加到备份列表中，并支持快速查找、过滤设置功能，在备份时过滤已选列表中暂时不需要备份的虚拟机。	
			针对 VMware 备份需能够支持海量虚拟机和数据量的环境，支持智能化备份任务管理：	
			1）支持 1 个灾备主控节点和执行节点集群，可以一个备	

			份策略选择多个执行节点，运行时由主控节点选择使用的资源，而不需要人工选择；	
			2）支持一个备份策略可以选择多个备份存储介质，也可以选择第三方存储介质；	
			3）支持 VMware 虚拟化主机、存储备份负载可配置，可以结合 VMware 主机和存储性能和负载情况配置不同主机和存储的备份并发任务数，降低对用户环境的性能影响；	
			4）支持 VMware 虚拟化快速挂载和回迁功能，快速挂载恢复可以将核心执行时间缩短到分钟级；支持回迁功能操作均在灾备系统管理页面上操作完成，回迁可以将快速挂载时新增的业务数据恢复到一个稳定运行的虚拟机。	
			支持华为 Fusioncloud、Openstack、、EasyStack、深信服、浪潮云、Zstack、云宏、华三云等主流云平台上数据的备份与恢复，支持无代理方式备份、LAN-Free 备份、完全和差量备份、海量虚拟机备份等。针对 OpenStack 云架构支持 Cinder、本地卷、Ceph 等存储模式备份。	
		容器数据备份	支持容器 Docker、容器云的数据备份与恢复，支持集群 Docker 镜像数据、配置文件定时备份，支持集群控制节点和重要节点整机备份，实现故障后整机恢复，支持完全备份、增量备份等方式	
		Hadoop 大数据平台数据备份	支持 Hadoop 生态系统中数据的备份和恢复，其中涉及的组件有分布式文件系统（HDFS）、分布式内存数据库（HBase）、数据仓库（Hive）；备份恢复支持 HBase 表和 Hive 表，备份及恢复的颗粒度更细，速度更快；支持完全备份和增量备份；支持 LAN-Free 备份；支持集群恢复；支持备份 HDFS 文件过滤设置：过滤文件、文件目录。	
		可信恢复	支持对备份对象指定非对称密钥进行数据加密，恢复时必须接入指定的密钥设备。	

		应急容灾功能	1. 可扩展支持自动/手动、一键容灾接管模式，当生产机宕机，系统支持自动、手动开启容灾机，接管生产机最新的数据和应用；	
			2. 支持实时备份数据、定时卷备份数据、云主机快照、虚拟化快照等类型数据作为灾备数据源，实现业务系统的应急接管，无需预先安装与生产机相同的操作系统和应用程序的方式；支持外置/内置容灾平台；可自定义设置容灾接管机的 CPU、内存、网络配置等相关参数。	
			3. 支持多种故障检测机制：可检测生产机应用、服务、进程、脚本、客户端代理等运行状态，当发生故障时，实现系统报警和自动接管	
			4. 支持容灾机任意时间点的容灾接管，当生产机出现故障后，可自定义输入任意时间点（RPO≤1 秒）进行接管，而非选择固定时间点进行应急接管，确保任意时间点接管后的应用正常运行	
			支持 SanBoot 功能，可通过 FC 或 iSCSI 网络把接管机所需的系统 LUN 和数据 LUN 送到物理服务器上启动后实现应急接管。	
			支持将执行同一业务功能的主机或有逻辑关联的主机以组的形式进行容灾接管和演练管理；支持设置业务组内主机启动顺序，可按业务逻辑顺序启动、关闭容灾系统中的接管/演练机群	
			支持一键式演练模式，支持任意时间点的主机演练：可自定义输入任意时间点（RPO≤1 秒）的接管演练，一键开启演练机，无需预先搭建相关测试环境，灾备系统按照设定的演练策略自动进行主机演练，演练模式不影响生产业务的正常运行	

			支持自动演练和演练报告：自动演练并生成独立演练网络，通过虚拟化平台构建独立虚拟化网络，使演练环境与生产环境网络不相互影响，自动进行系统日志校验、文件校验、服务校验、数据库脚本校验，保证数据可用性，演练完成后，根据演练时设定的校验项生成数据演练校验的报告，发送至管理员邮箱	
			支持容灾接管机的可视化操作管理，通过产品自身WEB界面来控制和操作容灾或演练机的操作系统桌面，而不是通过第三方工具如虚拟化客户端登录容灾或演练虚拟机进行操作。	
			支持本机/异机自定义数据回迁，可手动选择需要回迁的磁盘及分区。支持仅增量数据回迁功能：支持识别出接管后新增的数据，仅将新增的数据恢复到生产系统中，无需将接管前的数据恢复到生产系统中；支持渐进式回迁：迁移接管机数据，采用渐进式的回迁的方式，先获取接管机当前最新数据，然后进行迁移，直到迁移结束。在迁移过程中，接管机还会有新数据生成，需要再次迁移，再获取最新变化的数据进行迁移。循环进行，直到连续多次迁移时间较短时，手动结束回迁，确保接管机无数据产生以完成最后数据的迁移；该过程接管机业务中断时间不得超过30分钟。	
		远程保护	支持一对一、一对多以及多对一等多种异地灾备，最大限度满足多分支机构的异地数据灾备需求；并支持同步策略数据校验机制，支持本地恢复及异地恢复。	
			支持异地容灾接管功能，本地生产机数据实时备份并实时复制至异地灾备中心，当本地生产机宕机，可在异地实现任意时间点的应急接管，保障业务连续性。	
			支持智能限制备份与恢复所占用的网络带宽资源，从而确保数据备份与恢复时，最大限度减小对用户业务正常使用	

			的影响。
		双活复制	支持双活复制模式，即源端和目标端都处于 Open 状态，目标端系统时刻处于可读可写状态，目标端可以提供实时访问服务，遇到故障时不需要重新加载系统，实现分钟级业务接管。当源端发生物理损坏的时候，可以通过目标端进行数据和业务的恢复。支持源端在不停机的状态下实现同步过程的初始化，初始化过程中不需要人工干预，自动完成。
		数据自动校验	支持灾备数据自动校验、运维整合机制，支持备份数据的自动校验，可进行校验周期设置，需 MD5、CRC32、SHA1、SM3 等四种以上的校验方式
		运维审计	支持与 SNMP 运维平台进行整合，支持与 Syslog 审计平台进行整合
		优化机制	支持断点续传，当数据备份过程中出现链路中断，恢复正常后，可从上一次断点处继续增量传输数据，无需重新进行完整数据传输，确保灾备数据的传输效率和完整性。
			支持基于源端的备份数据压缩技术，确保最大限度的减少备份存储空间占用和带宽资源占用。
			支持基于源端和目标端的备份数据重复删除技术，支持全局重删，支持管道重删；实时保护及副本数据管理功能中源端到目标端数据传输过程中的数据重删，使得数据传输需求的带宽更窄，传输数据量更少，传输时间更快。
		数据加密传输与存储	数据加密与安全证书功能：数据进行备份时，可对备份对象使用国家密码局认定的SM4国产商用密码算法进行数据存储加密，并具备使用安全证书加密保护备份数据加密密钥的策略，对备份数据加密密钥进行再次加密，其基于国密 SM2 密钥算法和基于 SM3 签名算法用于加密和签名，数据恢复时必须接入安全证书 KEY 和口令，保障备份、传输、

			存储、恢复等过程的安全	
		统一管理	通过灾备集中管理将各灾备节点资源纳管后，统一提供备份与恢复、数据级容灾、灾难恢复演练、应用应急接管等安全服务能力。	
		组织机构管理功能	用户可以自行建立组织机构，对组织内的灾备系统进行统一管理	
		大屏监控模块	灾备平台能够提供独立的大屏监控展示的门户窗口界面；	
			通过收集各个灾备节点等数据信息，集中进行管理和分析，用于大屏展示。	
		统一视图	支持通过图标等形式按不同维度进行大屏动态展示，如：饼状图、柱状图、雷达图等，可显示灾备节点相关资源信息、客户端信息、灾备报表信息、报警信息、灾备作业信息、灾备数据量统计信息等内容。	
		系统安全性	支持用户口令、CA 数字证书认证、USBKey 等多因子认证技术登录，保障系统登录的安全性，避免弱口令模式下的安全风险。	
			支持三权分立管理模式，即：系统管理员、审计管理员、安全管理员三种管理员身份多权限、多角色管理。	
			支持以邮件、短信等方式向对应的管理员发送报警信息；支持控制台告警、指示灯告警、蜂鸣器告警，并提供日志功能记录备份的系统和用户操作日志。	
			支持 Agent 代理端安装环境检测：支持在安装时自动对所处安装环境进行自动检测，自动分析是否满足系统安装的需要。	
3	云堡	产品架	2U 标准架构硬件，独立一台物理硬件平台实现所有功能，	

	垒机	构	不再额外安装任何软件；	
			操作系统基于加固安全操作平台，为主机提供深度防御。	
		管理结构	B/S 架构，采用 HTTPS 方式远程安全管理，无需安装客户端；	
		网络接口	一台 2U 硬件平台中；	
			堡垒主机 4 个 100/1000M 自适应以太网口；	
			应用托管 4 个 100/1000M 自适应以太网口；	
		支持协议	字符型远程操作协议：SSH、TELNET；	
			图形化远程操作协议：RDP、VNC、XWIN	
			文件传输协议：FTP、SFTP；	
			通过应用托管中心支持对数据库远程操作协议：ORACLE、MSSQL、Mysql、DB2、SyBase、INFOMIX 等协议审计，支持各种数据库客户端（PLSQL/TOAD/SQLPLUS/OEMC/Powerbulider/DBACCESS/DB2CMD/Quest Central for DB2 等）的登录账号和密码自动代填功能；	
			通过应用托管中心支持其他访问协议：PCANYWHERE、AS400、Radmin、DameWare、KVM、HTTP/HTTPS 等，并提供账户名密码自动代填功能；	
		端口安全技术	采用端口安全机制，不开放或变相开放 3389、22、21、23、5900 等高危端口实现高效协议代理；	
		网络环境	运维口、设备口、热备口、数据口	
		RDP 协议代理	采用真正意义上的 RDP 协议级代理机制，而非经过多次应用级转换的“RDP 代理”，使得 RDP 运维代理最高效，单	

		技术	台设备即可实现 500 以上的 RDP 并发访问	
		认证方式	默认支持本地口令认证，支持第三方 radius 认证、LDAP 认证、AD 域认证、证书认证、混合认证、支持内置动态 Token 双因素认证、支持手机令牌认证；	
		批量操作	支持账号批量导入、导出、修改、删除等操作，支持直接从 AD 域批量导入用户账号；	
		用户分组	支持对用户进行无限级分组，便于管理；	
		安全机制	密码强度：可设置用户密码的强度要求，改密时必须符合设定的密码强度要求；	
			登录 IP 限制：可限制登录的 IP 地址范围；	
			防暴力破解：可以设置连续登录错误几次后，系统自动锁定帐号；	
			审计有效性：用户账号产生运维日志后不允许删除（可禁用）；	
		临时帐号	可基于有效期灵活创建各类临时帐号，到期禁用；	
		设备分组	支持对目标设备进行无限级分组，便于管理；	
		批量操作	支持目标设备的批量导入、导出、修改、删除等操作；	
		访问授权	支持细粒度的访问授权策略，可基于用户、用户组、设备、设备组、协议、支持 IP 地址范围、时间等进行灵活授权；	
		Html5 技术	设备访问支持 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件，即可实现对目标设备的快速运维；	
		调用本地客户端	RDP、SSH、Telnet 等协议支持调用本地客户端工具，如 mstsc、Xshell、putty、SecureCRT 等；	

		数据库本地客户端调用	针对数据库运维，支持调用本地的数据库管理工具，如 Plsql Developer、sqlplus 等，不依赖应用发布服务器；	
		移动终端	支持移动终端运维（如手机、iPad 等），通过移动终端登录堡垒机，即可看到有权访问的设备列表，点击相应目标设备可直接进行运维操作	
		运维工单	支持内置工单运维，操作员可根据工作需求临时申请设备运维工单，管理员审批后可直接运维，过期失效；	
		自动化	用户自身可创建自己的自动化任务，如自动巡检业务、脚本自动执行任务等；	
			支持任务审批功能，管理员可查看相关用户的任务详细，如脚本内容、执行范围、时间等，管理员可授权和驳回；	
			任务执行结果可视化展示，用户可查看自身相关的自动化任务执行结果；	
		黑白名单	支持针对数据库 sql 语句、文件传输、操作命令创建黑白名单规则，一个名单可包含命令集中的多个 sql 语句 / 命令，黑名单支持会话阻断、命令阻断和命令告警三级策略；	
		部门分权	支持无限级部门分权功能，本部门的运维管理员只能查看、管理本部门的用户和设备；	
		系统重启恢复技术	设备系统重启可保留用户当前的操作窗口及数据，重启完成后可继续此前未完成的操作；	
		单机部署	单台设备即可支持所有功能，采用物理旁路、逻辑串联的部署模式；	
		双机部署	支持高可用的 HA 双机部署，采用心跳线和数据线两条线路，确保数据无延时同步，支持对方存活检察和服务自动修复功能；	

		集群部署	支持自建集群部署，不依赖任何第三方设备，如 F5、单独的存储设备等，支持无缝横向扩展；	
		分布式集群	支持分布式集群部署，从而实现多地多机房分布式管理；	
		硬件需求	设备存储要求：	
			堡垒主机存储空间 1T；	
			应用托管中心存储空间 1T；	
			接口要求：	
			堡垒主机 4 个千兆电口；	
			应用托管中心 4 个千兆电口；	
			性能要求：	
			图形并发会话数 300；	
			字符型并发会话数 600；	
			可管理设备数量 100 台；	
4	核心交换	基本要求和性能	1、交换容量 19Tbps，包转发率 3240Mpps	需提供主备各一台，共计两台。
			2、支持主控引擎 2，业务槽位 6 个，	
			3、支持模块化风扇框，可热插拔，单个风扇框在线更换过程中，系统仍有独立风扇框保持运行，独立风扇框数 2 个	
			4、为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计；	
			5、支持并实配独立的硬件监控模块，控制平面和监控平面物理槽位分离，支持 1+1 备份，能集中监控板卡、风扇、	

			电源、调节能耗	
			6、支持横向虚拟化技术，将多台设备虚拟为一台设备，支持长距离集群	
			7、为了简化管理，支持纵向虚拟化技术，支持把交换机和 AP 虚拟为一台设备	
			8、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6	
			9、支持 GE/10GE 端口 200ms 大缓存；	
			10、支持真实业务流的实时检测技术，秒级快速故障定位	
			11、支持硬件 BFD/OAM，3.3ms 稳定均匀发包检测，非软件 BFD 实现方式；	
			12、支持 G.8032 标准环网协议，要求倒换时间≤50ms；	
			13、配置：双主控引擎、双交流电源、满配风扇框与风扇，配置 24 个千兆光口，24 个万兆光，48 个千兆电口，16 个万兆单模模块，4 根 3m 堆叠线缆。	
5	PACS 存储	基本要求和性能	1、实配 SAN 与 NAS 统一存储，配置 NAS 协议（包括 NFS 和 CIFS）、IP SAN 和 FC SAN 协议，不需额外配置 NAS 网关，存储操作界面同时支持块存储和文件存储功能	
			2、支持控制器扩展，最大支持 8 控	
			3、系统内总一级缓存容量配置 128GB，且任意控制器一级缓存容量 64GB（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache、SCM 等）	
			配置 4*10Gb ETH +8*1Gb ETH+8*16Gb FC（含万兆和 FC 接口光模块）；支持 16Gb FC、8Gb FC、32Gb FC、1/10/25Gb Ethernet 等，双控最大支持 40 个主机端口	
			4、支持 SAS SSD、SAS、NLSAS 硬盘，并支持混插	

			5、配置容量：可用容量 20T	
			6、支持 SAN 与 NAS 的一体化免网关双活，任意一套设备宕机均不影响上层业务系统运行（业务不中断）。支持双仲裁服务器配置，支持 FC 链路复制，SAN 双活支持双活流量分担，支持故障自动切换和回切	
			7、支持 RAID 1、RAID3、RAID 10、RAID50、RAID 5、RAID6	
			8、采用多核处理器，配置控制器处理器总物理核心数 36 核	
			9、支持高速缓存分区功能，保障关键业务资源使用，为应用系统提供存储服务质量支持	
			10、支持分级存储，能够以 512 KB～1MB 的热点颗粒度为单位进行自动分级调整，提供图形化的自动分层策略调整工具，能够对数据分层的时间窗口和分层方式进行调整，提高存储资源利用效率，即支持在特定的时间段（定时），开启 I/O 监控热点数据，自动进行数据迁移。	
			11、存储厂商提供专有多路径（非操作系统自带多路径）软件，提供故障切换和负载均衡功能，支持 Windows\Linux。	
6	云 HIS 数据库服务器	基本要求和性能	单台硬件配置：40 核、256G 内存、1.2TB 硬盘，支持 RAID0、1、10 可选缓存或 Flash 保护，主机带 2 口个千兆以太网卡，2 个万兆网口（含模块），2*16GB 单口 HBA 卡。	需提供主备各一台，共计两台
7	SAN 交换机	基本要求和性能	单台硬件配置：24 端口 16G 接口光纤交换机，激活 8 口	需提供主备各

				一台，共计两台
8	虚拟化存储阵列	基本要求和性能	单台存储配置如下：硬件：双控制器，128G 高速缓存（控制器自带），8 个 16Gb FC 接口，	需提供主备各一台，共计两台
			可用存储空间 8T。	
			支持读写 IOPS2600K	
			软件：SVOS 存储管理软件（不限容量许可）：存储基本管理软件，存储虚拟化软件（支持异构存储管理和整合），动态容量供应软件，动态多路径软件，虚拟分区软件，性能监控软件，数据重删/压缩功能，卷迁移软件；本地数据卷克隆&快照，RAID 存储复制管理；存储数据分层，无中断迁移，存储性能分析软件等服务；	
9	云边界防火墙	设备基本要求	采用专用多核硬件架构与专用 64 位安全操作系统；硬件设备可以机架安装；软件采用模块化结构设计，默认 SSL VPN 功能，IPSEC VPN 功能，上网行为管理，负载均衡，防病毒功能，入侵防御功能。可扩展 URL 过滤功能，沙箱功能，流量控制功能。端口数量 9 个 GE 接口，网络吞吐量 6Gbps，最大并发连接数 250 万，每秒最大新建连接数 12 万，VPN 隧道数 2000 条，SSL VPN 并发用户数，支持 1000 个，本次提供 8 个	
		带宽管理	支持两层八级管道嵌套，能够同时做到两个维度的流量控制	
		分层带宽管理	支持 IP、应用、角色方式的套嵌分层管理	
		SSL VPN 客户端	对登陆客户端进程、杀毒软件的端点安全检查	

		检测		
10	核心虚拟网络线路	基本要求	1000M	需提供主备两条

附件二：信息安全与保密承诺书

信息安全与保密承诺书

本人，[范斌]（身份证号码[320422197504200118]，住址[新城东苑一区 7-606]，联系方式[15306149889]）；

本人，[刘会平]（身份证号码[320482199010134996]，住址[常州市金坛区华达名都 31 栋甲单元 1002 室]，联系方式[17766238889]）；

本人，[蔡克俊]（身份证号码[320422197105300111]，住址[金水华都 3-1803]，联系方式[15306148800]）；

本人，[樊林波]（身份证号码[32048219760317621X]，住址[东门大街 1 号]，联系方式[13306148158]）；

本人，[杨文俊]（身份证号码[320482197604144914]，住址[颐和世家]，联系方式[18961110096]）；

本人，[张斌]（身份证号码[320482198705226518]，住址[吾悦华府 3 幢乙单元 2604 室]，联系方式[18915813385]）；

本人，[汤爱兵]（身份证号码[320422197006280119]，住址[左邻右里 11 甲 201]，联系方式[15306141998]）；

本人，[赵利华]（身份证号码[320422197304090110]，住址[望华新村 83 幢 202 室]，联系方式[15306143000]）；

本人，[陈玟伽]（身份证号码[320482199706140104]，住址[金源福地 14 栋]，联系方式[13306141997]）；

系[中国电信股份有限公司常州分公司]（以下简称“公司”）员工，本人保证上述个人信息真实，现就参与公司与金坛区卫生健康局（以下简称“甲方”）[常州市金坛区卫健信息化平台“5G+云计算”服务]（以下简称“项目”）过程中获知的甲方和/或甲方的上级公司、下属公司、关联公司以及上述主体的客户的保密信息，向公司及甲方作出以下承诺：

1. 本人确认已知晓，本承诺书所述“保密信息”包括但不限于以下内容：

1.1 国家秘密：指关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。具体范围包括但不限于《中国电信集团保密工作管理办法（暂行）》所列举的国家秘密。

1.2 商业秘密：指不为公众所知悉，能为甲方及其上级公司、下属公司、关联公司或上述主体的客户带来经济利益，具有实用性的技术信息和经营信息或甲方要求保密的各种信息和资料，其具体范围包括但不限于企业运营信息、会议纪要、发展策略、网络状况、电信产品信息、营销计划、技术信息、技术资料、系统及设备信息、人员构成、费用预算、利润情况、财务资料、合同信息、客户资料等。

1.3 用户信息：指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定用户身份或者反映用户活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。主要包括身份信息、业务/合作信息、通信信息、消费信息等。

（1）身份信息：

个人身份信息：包括个人用户的姓名、有效证件类别和证件号、证件登记信息（如地址等）、有效通信联系方式、装机地址、银行账户信息、各类特殊名单等；

单位身份信息：包括单位用户的名称、单位有效证件类和编号、联系人身份信息、有效通信联系方式、装机地址、单位授权书或单位证明、银行账户信息等；

代办人身份信息：包括代办人的姓名、有效证件类别和证件号、证件登记信息（如地址等）、有效通信联系方式等。

（2）业务/合作信息：

包括各类用户的业务登记资料、入网协议、业务申请/变更/终止协议、与单位客户签订的各类商业合作合同、业务招投标书等。

（3）通信信息：

通话详单、原始话单、用户定位（位置）信息、用户身份鉴权信息（用户的服务密码、用户登录各种业务系统的密码）、用户通信内容信息、用户通信录等。

（4）消费信息：

包括用户的业务号码（固定电话号码、宽带账号、移动电话号码等），使用通信服务订购的业务信息（套餐、增值业务信息等），综合级的账务信息（缴费信息、欠费信息、账户余额变动信息、账户信息）等。

（5）其它信息：

凡是未纳入上述四类，根据《中国电信集团保密工作管理办法（暂行）》、《中国电信江苏公司商业秘密保护管理办法》（中电信苏〔2009〕663 号）、《中国电信江苏公司用户信息安全保护管理实施细则》（中电信苏〔2017〕203 号）、《中国电信江苏公司数据安全管理制度（暂行）》（中电信苏〔2017〕216 号）等规定的保密信息，或可能与用户相关、能够单独或者与其他信息结合识别用户身份和涉及用户隐私的信息。

1.4 上述保密信息包括以文档、光盘、软件、图书、报表、函件、照片、录音带、录像带、磁盘、光盘、U 盘、移动硬盘、胶片等有形介质存在的信息、数据，也包括通过口头、网络等方式传递的无形介质存在的信息、数据等。

1.5 如甲方及其上级公司修订或新制订国家秘密、商业秘密、用户信息等方面管理办法的，本协议中有关保密内容的范围以修订后的管理办法为准。

2. 本人保证，对保密信息，承担如下义务：

2.1 严格遵守国家保密及相关法律法规、公司保密规章制度、甲方及其上级单位制订的各项有关国家秘密、商业秘密、用户信息等方面管理办法等（包括但不限于《中国电信集团保密工作管理办法（暂行）》、《中国电信江苏公司商业秘密保护管理办法》（中电信苏〔2009〕663 号）、《中国电信江苏公司用户信息安全保护管理实施细则》（中电信苏〔2017〕203 号）、《中国电信江苏公司数据安全管理制度（暂行）》（中电信苏〔2017〕216 号）），对保密信息履行保密义务。对于项目履行过程中所接触到的甲方的上级公司、下属公司、关联公司，以及上述主体的客户的保密信息，须履行同等保密义务并承担责任。

2.2 如发现保密信息泄露或得知任何第三方获得保密信息，应当立即采取有效措施防止泄密范围的进一步扩大，书面向公司及甲方报告，最晚不得迟于知晓保密信息泄露时起 60 分钟，并提供本人掌握的所有相关情况。

2.3 任何情形下，如发现保密信息操作存在不符合规范、流程、合同约定、岗位职责等情形的，本人须立即向有权的上级机构、甲方书面请示，在得到明确书面指示后方可继续操作。

2.4 接入甲方网络、系统时，须接受甲方对本人的终端操作行为的监控，同时履行甲方关于终端安全管理的相关要求。甲方如发现上述行为存在违法、违规情形，本人应当立即终止访问，接受调查，承担对应责任。违法、违规情形发现三次以上的，公司及甲方有权责令本人退出项目工作并接受处罚，由此给公司及甲方造成损失的，本人承担全部赔偿责任。

2.5 本人承诺不得有以下行为：

2.5.1 不得将保密信息出售、转让或者以其他方式披露或泄露给第三方；

2.5.2 保密信息仅用于与项目有关的用途，不得将保密信息用于项目以外的任何用途（包含擅自对保密信息进行加工后应用），除为执行项目目的外，不得对保密信息进行复制；未经公司、甲方共同书面同意，也不得利用保密信息进行新的研究、开发、利用；

2.5.3 不得违反工作规范与要求，采用远程登录、系统后台、代理服务器等方式进入甲方设备或系统，不通过刺探或者以其他不正当手段（包括利用计算机进行检索、浏览、复制等）获取与工作开展无关的保密信息。

2.6 如本人离职，将承担如下义务：

2.6.1 无论何种原因离开公司、本人与公司就离职补偿与赔偿等事宜是否达成了一致意见、公司是否依约实际支付了相关赔偿、补偿，本人均须至少提前一个月告知公司及甲方，且在离职前移交或按指示销毁所有掌握的保密信息。个人工作日记等记录中如含有保密信息的，须在离职前进行清退或销毁。

2.6.2 无论本人今后是否在公司继续任职，对于过程中获知的保密信息，均将继续承担上述保密信息的保密义务，不得将保密信息以任何方式向第三方披露、转让或许可使用，不利用保密信息获取利益，亦不利用该保密信息为其他与甲方有竞争关系的企业（包括自办企业）服务。

3. 如本人违反上述承诺、义务，构成违法、违规或侵犯他人权利而引致刑事追索、行政处罚、索赔或诉讼，本人承诺承担全部刑事责任、行政责任、民事责任，给甲方造成损失的，本人将承担由此给甲方造成的一切损失（包括但不限于直接损失、间接损失、诉讼费、律师费、公证费、调查费、和解费用等）。

承诺人（签字）：

[中国电信股份有限公司常州分公司]（盖章）

[2021]年[7]月[12]日

附件三：网络信息安全承诺书

网络信息安全承诺书

本单位郑重承诺遵守本承诺书的有关条款，如有违反本承诺书有关条款的行为，本单位承担由此带来的一切民事、行政和刑事责任。

一、本单位承诺遵守《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》及有关法律、法规和行政规章制度、文件规定。

二、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

三、本单位承诺严格按照国家相关法律法规做好本单位网站的信息安全管理工作，按政府有关部门要求设立信息安全责任人和信息安全审查员，信息安全责任人和信息安全审查员应在通过公安机关的安全技术培训后，持证上岗。

四、本单位承诺健全各项网络安全管理制度和落实各项安全保护技术措施。

五、本单位承诺接受公安机关的监督和检查，如实主动提供有关安全保护的信息、资料及数据文件，积极协助查处通过国际联网的计算机信息网络违法犯罪行为。

六、本单位承诺不通过互联网制作、复制、查阅和传播下列信息：

1、反对宪法所确定的基本原则的。

2、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

3、损害国家荣誉和利益的。

4、煽动民族仇恨、民族歧视，破坏民族团结的。

5、破坏国家宗教政策，宣扬邪教和封建迷信的。

6、散布谣言，扰乱社会秩序，破坏社会稳定的。

7、散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

8、侮辱或者诽谤他人，侵害他人合法权益的。

9、含有法律法规禁止的其他内容的。

七、本单位承诺不从事任何危害计算机信息网络安全的活动，包括但不限于：

1、未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

2、未经允许，对计算机信息网络功能进行删除、修改或者增加的。

3、未经允许，对计算机信息网络中存储或者传输的数据和应用程序进行删除、修改或者增加的。

4、故意制作、传播计算机病毒等破坏性程序的。

5、其他危害计算机信息网络安全的。

八、本单位承诺，当计算机信息系统发生重大安全事故时，立即采取应急措施，保留有关原始记录，并在 24 小时内向政府监管部门报告，并书面知会贵单位。

九、若违反本承诺书有关条款和国家相关法律法规的，本单位直接承担相应法律责任，造成财产损失的，由本单位直接赔偿。同时，贵单位有权暂停或停止提供托管服务、断开网络接入，直至解除双方间《网络安全技术支持服务协议》。

十、本承诺书自签署之日起生效并遵行。

合同编号：JSCZE2104901CGN00

单位盖章：

日　期：

常州市金坛区政府采购

中标（成交）通知书

编号：坛政采公[2021]0007号

中国电信股份有限公司常州分公司：

常州市金坛区卫健信息化平台“5G+云计算”服务项目经评委会评审，确定你单位为中标（成交）供应商，分包1中标单位:中国电信股份有限公司常州分公司 中标金额为：人民币捌佰万元整（￥8000000元）。相关事宜通知如下：

1、请贵公司持本通知书于2021年07月14日前到本项目采购单位(常州市金坛区卫生健康局)办理签订合同等相关事宜。

2、请按合同约定认真履约。履约结束后及时以书面形式向采购单位提请组织验收。

3、不能按时签订合同、履约的，请提前向采购单位及常州市金坛区政府采购中心说明。因你公司原因不能按时签订合同、履约的，应承担相应法律和经济责任。

常州市金坛区政府采购中心

2021年06月29日

友情提醒：通过网站打印（下载）的中标（成交）通知书可直接对外使用，不需要再到采购中心盖章。