运维服务外包合同书

项目名称：2022年信息系统及安全保障运维服务

甲　　方：武汉市第四医院

乙　　方：武汉光谷信息技术股份有限公司

签订地点：武汉市

签订日期：二0二一年

合 同 书

武汉市第四医院（以下简称：甲方）和 武汉光谷信息技术股份有限公司（以下简称：乙方），依据《中华人民共和国合同法》的规定，就2022年信息系统及安全保障运维服务项目（以下简称：工程）项目建设有关事宜协商一致，同意按下述条款和条件签署本合同（以下简称：合同）。

一、 合同文件

1、本合同附件包括招标文件、投标文件、中标通知书、双方工作会议备忘录等。以下文件均是本合同的组成部分，并互为补充和解释，如各部分存在冲突之处，甲方有权选择以下文件的优先级：

（1）招标文件；（2）投标文件；（3）中标通知书；（4）合同书；（5）双方工作会议备忘录。

2、本合同附件均作为本合同的组成部分，与本合同具有同等法律效力。

3、附件清单：

附件一：信息安全保密承诺函

附件二：外包业务工作考核表

附件三：廉洁承诺书

二、 服务期限

本合同服务有效期限为1年。起始时间为2021年12月20日，终止时间为2022年12月19日。

三、 服务范围

1、包含所有现有及未来根据业务需要增加的网络、服务器、存储、安全及配套系统运行维护保障服务。包括计算机网络系统、网络安全、服务器及存储系统、数据库系统等。

2、现有硬件内容包含网络通信及安全等设备共计302套（台），服务器和存储等设备共计89套（台），无线网络系统6台AC，896台AP，基础支撑软件平台包含虚拟化群集虚拟机403套（台），数据库64余个实例。

四、 服务内容

服务类别	序号	名称	描述	数量	服务
一、信息化系统运维服务	1	性能评估及深度优化服务	网络优化服务：提供每月一次全院的网络设备进行深度巡检，通过对历史流量、系统配置、运行日志等多个维度进行核查分析，并结合产品官方最新的最佳配置指南对网络设备部件微码版本、系统版本等给出最优升级建议，形成巡检优化报告并配合现场工程师进行系统配置调整及性能优化工作。	12次	每月一次主动巡检频度，提供全系统的主动巡检，优化服务，自动化服务等。【每月输出一份含在巡检报告中】
			服务器及存储系统优化服务：提供每月一次全院的服务器（含虚拟化）及存储系统进行深度巡检，通过存储空间使用情况，虚拟化资源分配情况，性能波峰波谷指标等多个维度进行核查分析，并结合产品官方最新的最佳配置指南对服务器部件微码版本、虚拟化版本、存储硬盘微码版本等给出最优升级建议，形成巡检优化报告并配合现场工程师进行系统配置调整及性能优化工作。		

			支撑环境优化服务：提供每月一次全院的支撑环境进行深度巡检，通过对操作系统、中间件、应用系统的运行日志、告警信息、用户反馈等多个维度进行核查分析，保障各组件正常协同工作，形成巡检优化报告并配合现场工程师进行系统配置调整及性能优化工作。		
	2	数据库系统技术服务	提供拥有OCP认证的数据库工程师承担全院等数据库的日常使用保障、运行监控、配置更改、故障排查、数据全量、增量备份服务，并提供每月一次的深度巡检，通过对配置文件、数据文件、日志文件、备份策略及备份情况进行健康性检查并进行优化，形成巡检优化报告。	1项	
	3	灾难恢复演练及数据保障服务	提供多名高级工程师定期对重要业务虚拟化进行模拟故障切换、备份虚拟机文件拉起运行测试服务，保障备份的虚拟机能够正常恢复，同时每年四次进行数据	4次	一级二级数据库还原演练，PACS图像数据抽查还原测试，一年四次。对虚拟化环境

			库还原演练、数据恢复测试，提供全流程的灾难恢复演练操作手册		和数据库制定相应备份策略，定期进行数据备份，并检查数据备份作业的情况。
	4	公司技术支持团队应急服务	提供不少于三名及以上高级工程师后台支撑服务，提供突发性、紧急事件的会诊和保障恢复等（包含服务器、小型机、网络、存储等系统）。	1项	提供不少于三名及以上专业高级工程师后台支撑服务，提供突发性、紧急事件的会诊和恢复等（包含服务器、小机系统、网络系统、存储备份系统系统分析及优化建议【每月输出一份含在巡检报告中】）
			针对医院新系统上线、设备迁移变更等情况、提供现场技术服务和技术保障，并协助新系统上线时相应的支撑环境系统调试。		医院有新系统上线或设备迁移变更、提供现场的技术服务和技术保障，并协助新系统上线时相应的支撑环境

					系统调试。
			提供7*24小时的技术支持服务，包含备品备件服务、现场支持服务。在质保期内的设备协助院方联系原厂进行维修或更换，过保的设备协助院方进行维修恢复（过保设备的维修费用据实结算）。		
	5	备品备件更换服务	1、提供原厂续保服务采购清单，详见下列“维保设备清单” 2、提供故障设备（未购买原厂保）维护，备品备件更换服务	1年	提供故障设备（未购买原厂保）维护，备品备件更换服务，备件维修和购买费用由医院单次购买，乙方提供更换服务。
	6	现场技术人员值守	提供一人/年的5*8小时驻场服务，以及7*24小时的响应服务： 1、提供信息资产统计服务，包含硬件设备型号、数量、版本等信息统计记录；软件产品型号、版本和补丁等信息统计记录；网络结构、网络路由、网络IP地址统计记录；综合布线系统结构图的绘制；其它附属设备的统	1人/年	

			计记录； 2、保证网络的实时连通和可用，保障接入交换机、汇聚交换机和核心交换机的正常运转； 3、主机、存储设备的日常监控，设备的运行状态监控，故障处理，操作系统维护，补丁升级等内容，硬件维护包括增加设备、卸载设备、更换设备、除尘等； 4、定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生； 5、处理并解决甲方临时的工作安排。		
二、安全运维服务	1	高级深度渗透测试服	提供医院网络安全高级深度渗透测试服务，检验网络安全防御体系的有效性，充	1项	《信息系统资产收集调研表》

		务	分暴露和发掘潜在的传统漏洞与业务逻辑漏洞，查找业务系统及承载其运行的基础环境存在的安全隐患，以明显直观的方式反映系统的安全现状。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试等；服务要求针对医院要过等保测评的业务系统（包括三级系统和外联的二级系统），提供每个业务系统一年一次渗透测试服务。		《渗透测试授权书》 《渗透测试报告》 《渗透性测试回归测试报告》
	2	蓝队评估服务（团队服务）	通过专业的高级攻防工程师组成蓝队，针对医院的系统、人员、软件、硬件和设备同时执行的多混合、基于对抗性的模拟攻击，以此来发现医院在系统、技术、人员和基础架构中的存在的隐患。用尽可能接近真实环境攻击的方法来模拟黑客 APT 攻击，从而发现有可能被黑客利用的安全漏洞，以此对目标网络安全状况进行评估的一种服务型业务。	1 次	《蓝队评估授权书》 《蓝队评估报告》

			主要测试方法包括： 1.服务网络渗透&应用程序渗透基础服务；网络渗透&应用程序渗透-->纵向渗透-->横向渗透-->撰写蓝队评估报告-->报告解读-->漏洞复测； 2.物理渗透测试：到客户现场开展身份识别绕过、本地信息嗅探、硬件系统漏洞、设备远控攻击、近源物理入侵等评估工作；以绕过身份识别、嗅探重要信息、获得系统权限、获得员工信息为目的； 3.社会工程学攻击测试：通过发送钓鱼邮件、鱼叉邮件、交友诈骗、水坑攻击以及其他社工方式；通过企业员工打开进入系统&内网的突破口； 4.开展伪造wifi钓鱼、问卷调查、虚假活动钓鱼等方式获取员工敏感个人信息；进而实现对医院内部网络的渗透工作。要求一年提供一次蓝队评估服务。		
	3	公司应急响应	1、提供三名业安全服务工程师后台支撑服务，当发生	1年	《应急响应报告》

		团队支持服务	重大的网络安全事件时（如外部黑客入侵、数据泄露、勒索病毒等突发安全事件等），2小时内赶至现场处理，处理手段包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响，最少提供2人到达现场，一名安服和数据分析工程师； 2、提供7*24小时技术支持服务，快速响应处理应急事故，如远程无法解决应在2小时内赶至事故现场处理；应急响应时间：全年7*24小时，在驻场人员无法解决问题时，二线专业响应服务，人员接到通知后2小时内到场； 3、备件备机响应：当医院现有的安全设备出现故障且无法修复的情况下，乙方提供临时的安全设备代替，并协助故障设备修复；		
	4	网络安全应急演练服	配合开展医院网络安全应急演练服务（一年2次），提供必要的技术支持服务，	1项	《安全漏洞扫描报告》 《攻防演习防

		务（团队服务）	包括制定应急演练方案设计、搭建演练环境、参与演练、协助编制演练总结，通过网络安全应急演练，提升医院整体的应急响应能力。并根据用户要求，配合开展医院应急演练等工作中的安全设备相关部分内容，以检验相互协调的应急响应能力，提升全员安全意识。		守成果报告》《重保时期安全值守日报》《重要时期安全保障服务方案》《重要时期安全保障服务工作总结》
	5	网络安全咨询服务	1、根据医院息安全管理体系基本要求，结合医院自身实际情况和需求，协助组织按照PDCA的过程，规划、建设、使用和维护信息安全管理体系。每半年进行方案修订与增补。 2、依据国家政策相关标准要求，对医院信息中心网络安全资产清单、网络安全拓扑图、 网络安全设备技术资料、网络安全策略进行梳理，并实时更新、制定网络安全规划、方案，建立医院网络安全保障体系。 3、日常安全咨询服务 4.综合医院网络安全需求，在深化信息化建设的基础上统筹规划、技术创新、同	1项	《规划一套网络安全保障体系》

			步建设，面向医院级网络空间安全，在“实战化、体系化、常态化”的指引下，通过持续监测、分析、响应，提升“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”能力，做到底数清、告警准、抓重点、见成效，打造包含“一平台、二网络、三能力”的融合网络安全产品与服务的医院级创新网络安全运营中心。		
	6	网络安全服务人员	提供一人/年的5*8小时驻场服务以及7*24小时的响应服务： 1、日常的安全设备物理检查，针对医院所有安全产品提供定期巡检、预防性维护、配置变更管理、资产清理、处理威胁预警、工作报告等；并协助用户技术人员及网络安全的技术人员完成补丁更新、漏洞更新等服务，每天定时查看基于态势感知系统的安全问题处理与处置； 2、依托于医院现有的安全设备，通过查看相关安全产品告警、安全播报、安全通	1人/年	《资产信息库列表》 《漏洞扫描报告》 《配置核查报告》 《新系统上线环境安全评估报告》 《安全检查整改解决报告》 《安全工作日志》 《网络安全状况月报》 《一套网络安全管理体系》

			告以及医院线下反馈，根据以上来源的威胁线索，核实威胁、追溯来源，并评估影响范围，最终提供安全处置建议，整理安全整改通告等； 3、通过数据挖掘和调研的方式确定医院全网内外网资产范围，对暴露在整个互联网上服务器和设备的端口、协议、应用，乃至漏洞进行纵深据挖掘和调研，来确定医院资产范围，并生成资产及应用列表； 4、在发生网络安全紧急事件时，第一时间协调各安全厂商、乙方二线专家支撑、医院相关负责人以及乙方相关技术力量进行问题处置，完成安全故障处理报告，并负责到底，最终结果向甲方负责人汇报，并形成各类问题处置文档汇总以备核查，同时修订完善网络安全制度； 5、协助进行网络安全迎检检查：协助医院信息中心开展检查工作，提前准备检查各项信息安全工作的落实		《内外网资产调研台账》

			情况，提升医院整体安全基线，根据检查提前完成自查，并完成自查报告，最终提出网络安全整改建议和整改办法，以便在正式检查之间整改； 6、协助进行网络安全宣传：协助医院信息中心提供安全意识服务，针对医院信息中心技术人员和管理人员提供网络安全培训，包括网络安全意识培训，网络安全技术培训，不限于网络安全等级保护培训、网络安全法培训、国内外网络安全形势、安全意识培训等。 7、协助进行新上线的重要业务安全评估：协助医院信息中心对新上线业务进行漏洞扫描、基线配置核查服务，根据信息中心实际需求提供新系统上线环境评估服务，最终编制安全评估报告，并协助进行整改。 9、驻场人员要求： 熟悉医院全部的安全产品，如：网闸、防火墙、WAF、IPS、漏洞扫描、准入设备、态势感知等；承担过安全运		

			维服务、重保服务、渗透测试服务、应急响应服务等类似安全服务项目； 在WEB安全、系统安全、移动APP安全技术领域中具备至少2年以上的渗透测试、安全评估相关工作经验，负责过相关项目，熟悉常见安全厂商产品安装配置，日常管理检查，并通过认证的高级网络安全工程师。 10、处理并解决甲方临时的工作安排。		

1、信息资源运维服务技术要求

（一）咨询规划服务内容

乙方组织专业团队针对甲方业务系统情况，基础设施环境，结合甲方当前用户量，数据量，和发展趋势提供整体的信息化发展规划设计建议和咨询服务。

包含针对数据中心计算资源，存储资源，网络资源，网络安全，备份容灾，院区网络架构、云计算平台的计算、存储、网络、安全、数据库、中间件架构设计；云计算平台迁移、扩容设计，等提供全方位的咨询设计服务。

（二）集成服务内容

乙方组织专业系统工程师团队，配合甲方新增设备，扩容等项目建设时，协助系统集成【不包含基础设备操作系统安装搭建，上架，物理连接等】，系统割接，联调等服务。同时包含针对设备或系统升级所衍生的数据迁移，系统移植等服务。充分保障甲方各系统平滑安全的升级和扩展硬件软件基础架构平台，保障新的设备增加和项目实施过程中业务系统的连续性和数据的安全性。

（三）运维服务内容

包括如下内容：

1、信息资产统计：此项服务为基本服务，包含在运行维护服务中，帮助我们对用户现有的信息资产情况进行了解，更好的提供系统的运行维护服务。建立设备台帐表，每月对设备进行一次现场定期巡检服务，巡检完毕后提交巡检分析数据报告。通过巡检过程中对系统的调整和优化，减少设备发生故障的概率，保证设备稳定、高效运行。

2、网络及网络安全运维：从网络的连通性、网络的性能、网络的监控管理三个方面实现对网络系统的运维管理。1、甲方终端信息点线缆的维护，对甲方桌面终端管理人员进行现场简单故障排查培训，及时更新维护资料及当月维护月报。2、甲方网络设备及系统的维护，定期完成网络设备配置数据的备份、整理、按需调整配置、设备清洗、紧急故障排除等。3、定期对网络安全设备进行检查，并出具安全日志报告，及时协助医院查找网络信息系统运行过程中的安全漏洞，并采取有效措施加以修补。

3、主机、存储系统的运维服：主机、存储设备的日常监控，设备的运行状态监控，故障处理，操作系统维护，补丁升级等内容。1、定期对服务器及存储系统进行日常维护、保养、更新、升级、巡检、故障检测排除，协助医院进行服务器及存储系统性能监测、配置优化、故障检测排除、用户管理、资源分配、安全性控制等。根据用户要求安装、调试并优化域控制器，数据库服务器，业务服务器，办公服务器等的连接配置，建立服务器系统常用应用软件及驱动程序库。

4、虚拟化平台运维：负责虚拟化平台的日常维护工作，主要包括安全管理、网络存储管理、高可用管理、数据备份与恢复管理、虚拟机管理等，使得VMware虚拟化产品得到更及时的故障响应和处理，保障医院生产系统的安全稳定运行

5、云计算平台运维服务：

1）控制台运维

通过控制台实现虚拟化监控、存储监控、网络监控等的信息集中展现，能够将不同数据源的性能数据进行整合，并进行集中展现，包括实时的性能数据和历史性能数据，并对不同监控源性能数据监控策略的灵活制定

2）从面向基础架构监控到面向服务转型

通过配置管理库和运维服务流程，实现运维管理的标准化、可计量、可追溯，提升运维服务管理效率和服务质量，使运维管理逐步由面向服务的管理模式转型。

具体服务内容包括不限于以下方面：

*服务监控技术：监控云计算平台的虚拟机、网络、数据库、应用状况，提供服务监控准确性、实时性、全面性的保障

*服务容量管理：测量服务的容量，规划服务的建设，扩容、迁移等工作

*服务性能优化：从各个方向，包括网络优化、操作系统优化、应用优化、客户端优化等，提高服务的性能和响应速度，改善用户体验

序号	服务模块	内容描述
1	性能监控	通过控制台进行统一监控管理，包含告警、资源、拓扑和性能，协助用户进行快速定位和处理故障
2	虚拟机监控	提供虚拟机告警、资源、拓扑和性能等全方位监控能力，帮助用户对于云资源保障问题进行定界定位。
3	应用监控	以应用的视角来监控资源，从容量，负载等各个方面对应用的资源使用情况进行持续的评估，针对关键业务进行全方位的保障。
4	告警设置	提供多种机制针对不同场景提供相应的手段进行告警，使得故障定位更精准，提升运维效率
5	日志管理	收集并管理日志，用于对系统的运行状况进行了解，排障，遭遇故障事件时的问题定位。
6	系统备份	要备份各服务实例数据，以便服务实例在出现异常情况时能够快速恢复数据
7	系统恢复	当但服务实例异常，导致服务实例无法正常使用时，需要选择相应的备份文件进行数据恢复。常见的恢复场景如下： 1、**恢复至某个时间点：**将服务实例数据恢

		复至某个时间点的状态。定时方式备份的文件 2、**恢复至服务实例升级前的数据：**当服务实例升级失败需要回退到升级前状态时，可利用备份数据进行恢复。手动方式备份的文件 3、**恢复至重大业务调整前的数据：**重大业务调整可能导致服务实例出现故障，利用备份数据可将服务恢复至重大业务调整前的状态。手动方式备份的文件
8	故障处理	以尽快恢复系统为原则： 定位故障时，应及时采集故障数据信息，并尽量将采集到的故障数据信息保存在移动存储介质中或网络中其它计算机中。 在确定故障处理的方案时，应先评估影响，优先保证业务的正常传送。

6、数据库系统运维服务：

提供的数据库运行维护服务是包括主动数据库性能管理，数据库的主动性能管理对系统运维非常重要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。

提供的数据库运行维护服务还包括快速发现、诊断和解决性能问题，在出现问题时，及时找出性能瓶颈，解决数据库性能问题，维护高效的应用系统。

数据库运行维护服务，主要工作是使用技术手段来达到管理的目标，以系统最终的运行维护为目标，提高用户的工作效率。

为甲方数据库的日常维护、运行监控、补丁升级、优化、数据备份、恢复、故障恢复服务，同时提供每月巡检服务。

具体数据库运行维护监控的基本服务内容包括：

序号	服务模块	内容描述
1	Oracle 数据库 7*24 电话支持服务	每周 7 天，每天 24 小时支持中心电话，电子邮件答询，以满足业务发展的需要。 Oracle 产品技术专家直接同客户对话，帮助解决客户提出的疑难问题。 根据问题的严重程度，将优先解决客户认为是关键而紧急的任务。 对客户提出的一般性问题进行技术咨询、指导。 定期的客户管理报告，避免问题再度发生。
2	Oracle 数据库产品 现场服务响应	数据库宕机 数据坏块 影响业务不能进行的产品问题 软件产品的更新及维护。
3	Oracle 数据库产品 系统健康检查	对系统的配置及运作框架提出建议，以帮助您得到一个更坚强可靠的运作环境 降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张 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 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 协助进行数据库空间的规划管理 检查数据库备份的完整性 监控数据库性能 确认系统的资源需求 明确您系统的能力及不足

序号	服务模块	内容描述
		优化 Oracle Server 的表现 通过改善系统环境的稳定性来降低潜在的系统宕机时间
4	Oracle 数据库产品 性能调优	分析用户的应用类型和用户行为 评价并修改 ORACLE 数据库的参数设置 评价并调整 ORACLE 数据库的数据分布 评价应用对硬件和系统的使用情况，并提出建议 利用先进的性能调整工具实施数据库的性能调整 培训用户有关性能调整的概念 提供用户完整的性能调整报告和解决方法

7、数据备份服务：

根据不同的应用要求，对虚拟化平台和数据库数据进行备份，不同的应用服务器和数据库要求制定不同的备份方案，合理使用备份软件，达到备份的效果，实现 D2D2T 的备份要求，并定期对备份数据进行归档保存。

8、数据库还原演练：

乙方组织定期对备份的数据进行还原测试，验证备份数据的可靠性，完整性和可用性。

9、应用服务运维服务

应用系统日常维护管理和监控工作，提高对应用服务平台事件的分析解决能力，确保平台持续稳定运行。

应用服务平台监控指标包括配置信息管理、故障监控、性能监控：

*执行线程：监控配置执行线程的空闲数量。

*JVM 内存：JVM 内存曲线正常，能够及时的进行内存空间回收。

*连接池：连接池的初始容量和最大容量应该设置为相等，并且至少等于执行线程的数量，以避免在运行过程中创建数据库连接所带来的性能消耗。

*检查日志文件是否有异常报错

*如果有集群配置，需要检查集群的配置是否正常。

应用系统业务服务：

*支撑软件、业务系统软、件应用管理软件和与之相关配套内容的综合运行维护和配套服务；

*数据共享交换和与之相关配套的综合运行维护和配套服务；

*应用协同服务

*互联互通测评的配套服务等、数据质量基础综合运行维护和配套服务和数据质量标准化综合运行维护和配套服务

10、7*24小时在线值班：7*24小时的在线支持服务能力，乙方组织工程师要求立即响应用户服务请求提供远程支持，如一线工程师不能解决问题或诊断有硬件故障，二线工程师2小时内到达现场，并派出获得原厂商资格认证的服务工程师立即赶赴故障现场进行紧急现场支持。硬件故障报修厂商，走对应的原厂备件服务流程。

11、备品备件及设备维修：提供主要设备（网络、X86服务器、小型机、存储）易损件的备品备件，保障甲方主要设备的正常运行，并在出现故障后48小时内提供应急备件；乙方负责出具故障设备的维修处理建议并报甲方批准，甲方根据情况可交由乙方或任意的第三方进行维修处理。乙方处理过程中如因设备过保所产生的所有费用(维修、更换、物流等)由甲方承担，费用按次结算，乙方并负责设备维修后的正常恢复上线。

12、用户现场技术人员值守（1名、5*8小时的驻场服务，以及7*24业务响应服务）

1、提供长期的用户现场技术人员值守服务，保证医院支撑环境的连通和可用行，保障医院个业务平台的正常运转。现场值守的技术人员每天记录支撑环境的运行状态，进行整体性能评估，针对资源的利用率进行优化并提出资源扩容和优化的建议。

现场值守人员还进行数据库及中间件的日常运行状态的监控，对各种应用服务日志检查，对重点事件进行记录，对事件的产生原因进行判断和解决，及时发现问题，防患于未然。形成报表进行统计分析，便于进行支撑环境的分析和故障的提前预知。

2、运行分析与管理服务

运行分析与管理服务是指工程师通过对运行状况、问题进行周期性检查、分析后，

为提出指导性建议的一种综合性高级服务，其内容包括：

服务内容	服务优点
向客户提供专家电话号码。	保证重大问题第一连线至专家。
每月向客户提交CASE汇总分析报告	使客户了解历史故障情况以及故障预防建议，最大程度减少故障隐患，更高效的进行管理。

13、原厂续保服务采购清单：

序号	类别	描述	数量
1	原厂服务维保	四台HDS G200存储维保：7 x 24 x 365一小时电话响应；紧急情况时，两小时赶赴现场处理问题。维护及微码升级；备件更换；自动报警；远程诊断及支持；每月一次定期巡访并进行设备维护	1年
2		黑盾流控设备包含一年的URL库，应用特征库及软件固体升级，含一年技术支持（2台）	1年
3		东院+西院准入，盈高 ASM6305（2台）	1年
4		联想flex刀箱+6块刀片服务器(1套)	1年
5		联想X3850X6服务器(4台)	1年

2、安全运维服务技术要求

1、渗透测试服务

提供武汉市第四医院网络安全渗透测试服务，检验网络安全防御体系的有效性，充分暴露和发掘潜在的传统漏洞与业务逻辑漏洞，查找业务系统及承载其运行的基础环境存在的安全隐患，以明显直观的方式反映系统的安全现状。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中

间人攻击、web脚本渗透、B/S或C/S应用程序测试等。

乙方需提供专业的渗透测试人员，采用自主知识产权的代码检测工具，对武汉市第四医院提出业务系统进行渗透测试，出具《武汉市第四医院系统渗透报告》、《武汉市第四医院系统渗透复测报告》，并协助网络安全整改工作，切实提升武汉市第四医院网络安全渗透报告网络安全防御能力。

交付成果：

《武汉市第四医院系统渗透报告》

《武汉市第四医院系统渗透复测报告》

2、蓝队评估服务

通过专业的高级渗透工程师组成蓝队，针对武汉市第四医院目标系统、人员、软件、硬件和设备同时执行的多混合、基于对抗性的模拟攻击，以此来发现武汉市第四医院在系统、技术、人员和基础架构中的存在的隐患。用尽可能接近真实环境攻击的方法来模拟黑客APT攻击，从而发现有可能被黑客利用的安全漏洞，以此对目标网络安全状况进行评估的一种服务型业务。

评估点包括：

系统：深入的蓝队攻击将测试并暴露多个领域的漏洞。

整体信息化架构防护能力：网络、应用、路由器、交换机、电子设备等。

人员：职工、独立承包商、乙方、部门和业务合作伙伴等。

物理：IOT设备、门禁、智能终端等。

安全监控能力：日志保存、审计能力、APT攻击发现响应能力

蓝队攻击测试的模式永远不是使用千篇一律的方法，而是基于医院的规模、范围、行业、业务性质、法规要求和其他独特的安全特性来量身定制的。

总体工作流程分为：需求确认、签署授权、纵向渗透、横向渗透、成果确认等五大方面。

交付成果：

《蓝队评估测试授权书》

《蓝队评估测试报告》

3、公司应急响应团队支持服务

利用武汉市第四医院部署的态势感知系统，实现对全院安全态势分析，研判、处置，形成安全问题处置闭环。

提供多名专业安全服务工程师后台支撑服务，当发生重大的网络安全事件时（如外部黑客入侵、数据泄露、勒索病毒等突发安全事件等），1时内赶至现场处理，处理手段包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响，最少提供2人到达现场，一名安服和数据分析工程师；

提供7*24小时技术支持服务，快速响应处理应急事故，如远程无法解决应在2小时内赶至事故现场处理；应急响应时间：全年 7*24 小时，在驻场人员无法解决问题时，二线专业响应服务，人员接到通知后2小时内到场；

备件备机响应：当医院现有的安全设备出现故障且无法修复的情况下，乙方提供临时的安全设备代替，并协助故障设备修复。

交付成果：

《应急响应报告》

4、新系统上线基础环境评估服务

在医院中，基础环境比较复杂，存在的设备也比较多，如何在这些纷繁复杂的系统、设备、网络、终端中能够及时掌控基础环境情况，对于信息安全来说尤为重要。运维单位需利用漏扫工具对相关资产进行全方位扫描并出具漏洞扫描报告及分析。同时采用最佳配置核查实践对操作系统、数据库、中间件、网络设备、网络安全设备、网络边界进行配置核查。

交付成果：

《基础环境评估报告》

5、网络安全培训服务

网络安全宣传周形式为用户提供安全意识服务，针对武汉市第四医院信息中心技术人员和管理人员提供网络安全培训，包括网络安全意识培训，网络安全技术培训，不限于网络安全等级保护培训、网络安全法培训、国内外网络安全形势、安全

意识培训等。

6、网络安全应急演练服务

配合开展武汉市第四医院网络安全应急演练服务，提供必要的技术支持服务，包括制定应急演练方案，参与演练，协助编制演练总结，通过网络安全应急演练，提升武汉市第四医院整体的应急响应能力。根据用户要求，配合开展武汉市第四医院应急演练等工作中的安全设备相关部分内容，以检验相互协调的应急响应能力，提升全员安全意识。

交付成果：

《武汉市第四医院网络安全应急演练记录》

《武汉市第四医院网络安全应急演练总结报告》

7、网络安全咨询服务

1）、根据武汉市第四医院息安全管理体系基本要求，结合医院自身实际情况和需求，协助组织按照 PDCA 的过程，规划、建设、使用和维护信息安全管理体系。每半年进行方案修订与增补。

2）、依据国家政策相关标准要求，对武汉市第四医院信息中心网络安全资产清单、网络安全拓扑图、 网络安全设备技术资料、网络安全策略进行梳理，并实时更新、制定网络安全规划、方案，建立武汉市第四医院网络安全保障体系。

3）、提供日常安全咨询服务

4）、综合医院网络安全需求，在深化信息化建设的基础上统筹规划、技术创新、同步建设，面向医院级网络空间安全，在“实战化、体系化、常态化”的指引下，通过持续监测、分析、响应，提升“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”能力，做到底数清、告警准、抓重点、见成效，打造包含“一平台、二网络、三能力”的融合网络安全产品与服务的医院级创新网络安全运营中心。

交付成果：

规划一套网络安全保障体系

8、网络安全服务人员

提供一人/年的5*8小时驻场服务以及7*24小时的响应服务：

1、日常的安全设备物理检查，针对医院所有安全产品提供定期巡检、预防性维护、配置变更管理、资产清理、处理威胁预警、工作报告等；并协助用户技术人员及网络安全的技术人员完成补丁更新、漏洞更新等服务，每天定时查看基于态势感知系统的安全问题处理与处置；

2、依托于医院现有的安全设备，通过查看相关安全产品告警、安全播报、安全通告以及医院线下反馈，根据以上来源的威胁线索，核实威胁、追溯来源，并评估影响范围，最终提供安全处置建议，整理安全整改通告等；

3、通过数据挖掘和调研的方式确定医院全网内外网资产范围，对暴露在整个互联网上服务器和设备的端口、协议、应用，乃至漏洞进行纵深据挖掘和调研，来确定医院资产范围，并生成资产及应用列表；

4、在发生网络安全紧急事件时，第一时间协调各安全厂商、乙方二线专家支撑、医院相关负责人以及乙方相关技术力量进行问题处置，完成安全故障处理报告，并负责到底，最终结果向甲方负责人汇报，并形成各类问题处置文档汇总以备核查，同时修订完善网络安全制度；

5、协助进行网络安全迎检检查：协助医院信息中心开展检查工作，提前准备检查各项信息安全工作的落实情况，提升医院整体安全基线，根据检查提前完成自查，并完成自查报告，最终提出网络安全整改建议和整改办法，以便在正式检查之间整改；

6、协助进行网络安全宣传：协助医院信息中心提供安全意识服务，针对医院信息中心技术人员和管理人员提供网络安全培训，包括网络安全意识培训，网络安全技术培训，不限于网络安全等级保护培训、网络安全法培训、国内外网络安全形势、安全意识培训等。

7、协助进行新上线的重要业务安全评估：协助医院信息中心对新上线业务进行漏洞扫描、基线配置核查服务，根据信息中心实际需求提供新系统上线环境评估服务，最终编制安全评估报告，并协助进行整改。

9、驻场人员要求：

熟悉医院全部的安全产品，如：网闸、防火墙、WAF、IPS、漏洞扫描、准入设

备、态势感知等；承担过安全运维服务、重保服务、渗透测试服务、应急响应服务等类似安全服务项目；

在WEB安全、系统安全、移动APP安全技术领域中具备至少2年以上的渗透测试、安全评估相关工作经验，负责过相关项目，熟悉常见安全厂商产品安装配置，日常管理检查，并通过认证的高级网络安全工程师。

10、处理并解决甲方临时的工作安排。

交付成果：

《资产信息库列表》

《漏洞扫描报告》

《配置核查报告》

《新系统上线环境安全评估报告》

《安全检查整改解决报告》

《安全工作日志》

《网络安全状况月报》

《一套网络安全管理体系》

《内外网资产调研台账》

五、 服务方式

1、电话响应

设立7*24的值班响应电话，客服热线：400-687-4109（7×24小时服务热线）。

并安排有经验的工程师接受申告。出现故障时，医院通过指定的值班响应电话进行报障。当乙方需要查阅相关资料再对医院的问题进行回复时，对于一、二级故障确保在30分钟内回复，三级故障将在两小时内进行回复。

对于一级故障，乙方应在初步判断故障后马上派工程师赶赴现场。.

2、远程支持服务

对于通过电话指导不能解决的故障，在征得医院同意后，应通过远程接入手段，登录到故障设备，进行故障诊断，查找故障出现的原因，指导现场维护人员处理故障。

医院为乙方提供如下支持条件：

1 提供必要的远程技术支援的环境。保证安全管理功能，能防止非法登陆以保证设

网络安全。

2 服务人员远程登陆后，通过诊断，分析故障产生的原因，制定故障解决技术方案后，应电话通知医院，待技术方案经医院批准（医院批准的时间不包含在承诺的服务等级时间内）后，才能进行故障解决方案的具体实施。

3、现场服务

对于通过电话支持和远程支持都不能解决的设备故障，乙方应迅速提供现场支持服务，安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案，并最终排除故障。

1 服务人员在进行现场支持服务前应作好以下准备：

A 查阅医院用户档案，了解用户设备运行情况及设备以往所发生过的问题及处理办法；

B 准备技术服务工具、技术服务资料、交通工具、必要的软件。

2 服务人员抵达医院用户现场，首先提交《技术服务申请》给用户负责人签字确认。

3 了解设运行情况，核实故障现象，并根据故障现象进行故障分析、测试、诊断，并制定业务恢复和故障解决技术方案。 乙方须保证优先实施业务恢复，在恢复业务的前提下，再进行彻底的故障修复。

4 服务人员在处理故障后，要向医院维护人员解释故障原因和解决方法，以及在日常维护中的预防措施。

5 服务人员在处理故障时，要认真填写《故障处理报告》，并在离开现场前交医院客户主管部门存档，同时加入乙方的用户故障处理数据库备查。

6 在故障处理完毕后，服务人员须得到医院客户主管人员的同意后方可离开现场。

4、定期巡检

乙方向甲方提供每 1 个月一次的预防性巡检维护服务，在约定的时间内，指派固定的服务工程师对网络设备、服务器、存储、数据库及安全设备进行数据采集和分析，发现问题现场及时解决，并在一周内将系统分析维护报告提交给乙方相关负责人，以保证系统运行在最佳状况。

5、驻场服务

提供 5*8 及特殊时间现场驻场服务。

六、 服务等级协议(SLA)

1、信息资源信息服务要求

乙方保证每日1次按时巡检，并提供不限次的7×24小时现场、远程、电话、邮件等支持服务，并按照要求按时提供服务报告：

- 月度巡检报告：每月针对所有巡检内容的汇总报告；
- 年度总结报告：年底针对全年运维服务工作总结汇报；
- 不定期的技术服务报告：在接到采购人非定期巡检时间内的服务请求时，需要提供不定期的技术服务报告；

报告提交时间：每个月月底提交上一个月的服务报告，如遇节假日，时间顺延到下一个工作日17：30前。

乙方按照下列对故障级别、响应时间、服务到达时间及故障排除时间的定义来完成支持服务。

(1) 故障级别定义

级别定义	故障影响描述
一级故障P1	现有网络、应用等已经无法使用，或对用户的业务运作有重大影响。
二级故障P2	现有网络、应用等操作性能严重降级，或由于其性能失常严重影响用户业务运作。
三级故障P3	现有网络、应用等操作性能受损，但大部分业务运作仍可正常工作。
四级故障P4	在产品功能、安装或配置方面需要信息或支援，但对用户的业务运作几乎无影响，或根本没有影响。

(2) 故障的最长排除时间定义

如需现场故障处理的，故障排除时间是工程师到达用户现场开始计算。

故障级别	一级故障 P1	二级故障 P2	三级故障 P3	四级故障 P4
故障排除时长	2小时	8小时	10小时	18小时

2、安全运维服务要求

乙方保证每日1次按时巡检，并提供不限次的7×24小时现场、远程、电话、邮件等支持服务，并按照要求按时提供服务报告：

- 月度巡检报告：每月针对所有巡检内容的汇总报告；
- 年度总结报告：年底针对全年运维服务工作总结汇报；

- 不定期的技术服务报告：在接到采购人非定期巡检时间内的服务请求时，需要提供不定期的技术服务报告；

报告提交时间：每个月月底提交上一个月的服务报告，如遇节假日，时间顺延到下一个工作日17：30前。

乙方按照下列对故障级别、响应时间、服务到达时间及故障排除时间的定义来完成支持服务

(1) 网络安全事件分级定义

级别定义	故障影响描述
特别重大事件（一级）	是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受特别严重的系统损失；产生特别重大的社会影响。
重大事件（二级）	是指能够导致严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失；产生重大的社会影响。
较大事件（三级）	是指能够导致严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失，一般信息系统遭受特别严重的系统损失；产生较大的社会影响。
一般事件（四级）	是指不满足以上条件的信息安全事件，包括以下情况：会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

(2) 故障的最长排除时间定义

如需现场故障处理的，故障排除时间是工程师到达用户现场开始计算。

故障级别	一级故障 P1	二级故障 P2	三级故障 P3	四级故障 P4
故障排除时长	2小时	8小时	10小时	18小时

3、故障响应时间要求

根据故障对业务系统的影响程度分为四个级别：

在事件处理过程中，对于事件有分派时间限制和解决时间限制，以保证事件处理过程的高效运行。如果该事件的分派、解决超过了时限，需要通告事件经理，同时也要根据具体情况通告给其他相关管理人员。

分派二线时限指的是事件登记到转给二线所经过的时间；

解决时限指的是事件登记到事件状态变为“已解决”所经过的时间；

关闭时限指的是事件从“已解决”到“关闭”所经过的时间；

在事件管理流程中，不同的事件优先级对应了不同分派时限及解决时限，具体如下：

序号	优先级	一线响应时限	分派二线时限（分钟）	解决时限（小时）	事件关闭时限（工作日）
1	一级	立即	5	2	5天
2	二级	立即	10	8	10天
3	三级	立即	15	10	15天
4	四级	立即	30	18	15天

七、 项目组织

乙方为提高对武汉市第四医院_2022年信息系统及安全保障运维服务项目_的服务总体质量，为保障武汉市第四医院系统的正常高可靠持续性的运行，特成立项目专项小组，同时保证项目人员稳定。项目组成员见下表：

序号	姓名	专业	所在公司及职务	联系方式	执职业资格证明	在项目中担任的角色
		一、项目领导小组				
1	刘彬	项目管理、系统运营主机、存储、操作系统专家	分管副总	18986239916	项目经理	项目领导小组成员
		二、项目实施小组				

2	彭勇	主机、存储、备份系统领域技术支持服务	项目经理	18627135313	项目经理 信息系统项目管理师 HCIE-network、OCP、VCP	项目技术负责人
4	徐浩	主机、存储、备份、虚拟化、云计算机系统领域技术支持服务	项目经理	13329713317	项目经理 HCIE-network	一线工程师
5	彭建平	网络及服务器与存储、主机、存储虚拟化云计算系统技术维护现场服务	一线工程师	13626887331	一线服务工程师 OCM	一线工程师
6	张文俊	网络及服务器与存储	一线工程师	17764005770	一线服务工程师 HCNP-network	一线工程师
7	张玺	安全设备维护现场服务	一线工程师	17735905711	一线服务工程师 CISP	一线工程师
8	程洋	重保服务、渗透测试服务、应急	二线工程师	18163550446	高级	项目小组成员

		响应服务				
9	童爽	重保服务、渗透测试服务、应急响应服务	二线工程师	15871508979	高级	项目小组成员
10	胡鑫	重保服务、渗透测试服务、应急响应服务	二线工程师	18297558812	高级	项目小组成员
11	陈诺	网络及服务器与存储	二线工程师	17362678580	高级	项目小组成员
12	陈哲	数据库维护现场服务	二线工程师	19945055740	高级	项目小组成员
13	黄冬林	主机、存储、虚拟化技术维护现场服务	二线工程师	13037199820	高级	项目小组成员
14	张波	网络及服务器与存储领域技术支持服务	二线工程师	18627049300	高级	项目小组成员
15	吴婷	负责项目的服务质量跟踪、用户满意度	服务台主管	18672754757	高级	项目小组成员

		调查、服务改进计划与实施匹配				
16	邹敏	备件管理、第三方UC合同管理	备件管理经理	13607177636	高级	项目小组成员
17	杨梦婷	呼叫中心客服人员呼叫请求、记录、触发工单以及负责整个项目的文档收集、整理、符合性审查	服务台客服工程师	15927232883	中级	项目小组成员

服务投诉方式：027-81970707、4006874109

八、 合同金额及付款方式

1、合同总金额为人民币大写：**壹佰玖拾万零伍仟伍佰元整**，人民币小写：**¥1,905,500.00**。服务期内实行按半年付款，经甲方认可，每完成半年服务内容后30个工作日内支付合同总金额的50%。合同条款已审核，北文海

2、考核要求：甲方每半年对乙方进行工作考核评价(见附件二)，从服务态度、服务能力、服务质量、服务效率、服务纪律等5个方面进行考核打分评定，每方面考核内容分值20分，合计满分100分，得分大于等于90分为合格，该半年度维保费全额计算，得分 80-89 分为基本合格，该半年度维保费按每低于 90 分 1 分扣减1%；得分小于80分为不合格，该半年度维保费按每低于90分1分扣减1%；考评不合格，甲方有权解除服务合同。

九、 保密条款

参照附件一《信息安全保密承诺函》执行。

十、 争端的解决方法

甲方有权对乙方人员进行试用考核，服务工程师先通过甲方的面试和一个月的试用考核，面试及考核合格后正式服务项目。不能达到甲方要求必须无条件更换，如乙方服务不能达到甲方要求，甲方有权解除合同。

甲方未按本协议约定及时足额支付服务费用，每延迟一日，按应付未付款项的万分之二向乙方支付违约金，最高不超过本合同金额的百分之五；逾期付款超过 10 日的，乙方有权终止服务，并要求甲方赔偿由此给乙方造成的损失。

乙方未按要求履行合同所要求的服务时，甲方有权终止合同，由此造成甲方和最终用户的经济损失由乙方承担。乙方如不能按照合同约定期限完成项目，每逾期一天，以合同总金额为基数向甲方支付滞纳金，标准为每日按违约总额的万分之二累计，最高不超过本合同金额的百分之五。

双方本着长期友好合作的精神，协商解决本合同履行过程中的问题及纠纷。因本合同履行引起或与本合同有关的任何争议，如双方无法协商解决，任何一方可向甲方所在地的人民法院提起诉讼。

十一、 适用法律

本合同应按照中华人民共和国的现行法律进行解释。

十二、 合同生效

本合同经双方法定代表人或授权代理人签字盖章后生效。

十三、 其他

本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

十四、 服务交付

1、信息资源运维

1）、主动式巡检报告

交付时间：每月巡检结束后三个工作日提交

交付物：《运行维护与技术支持服务月度报告》包含《设备台帐》、《oracle 数据巡检表》、《硬件配置表》、《数据库配置表》、《系统配置表》、《网络设备日常巡检报告》、《服务器系统日常巡检报告》、《存储及备份系统巡检报告》、《维保设备现场服务月报》、《支撑环境运行维护与技术支持服务月度报告》包含《支撑设备台帐》、《支撑环境虚拟机、网络、数据库、应用运行状态月报》、《支撑环境备份报告》、《支撑环境优化建设报告》等表样清单；

2）、被动式服务：远程支持服务及现场服务

交付时间：现场服务报告单当场交付，并同时录入到每月月报中；远程支持服务每月附在月度报告中；

交付物：远程服务结束后交付《远程支持》报告单，现场服务结束后交付《客服现场服务报告》，远程支持及现场服务将按月在月度总结中统计。

3）、云支撑环境驻场人员

交付时间：每日提交日志类。

交付物：《支撑环境工作日志》

2、安全运维服务

1）、渗透测试服务

交付时间：服务要求针对医院要过等保测评的业务系统（包括三级系统和外联的二级系统），　提供每个业务系统一年一次渗透测试服务。

交付物：《武汉市第四医院系统渗透报告》、《武汉市第四医院系统渗透复测报告》

2）、蓝队评估服务

交付时间：根据院方要求时间一年提供一次蓝队评估服务。

交付物：《蓝队评估测试授权书》、《蓝队评估测试报告》

3）、网络安全应急演练服务

交付时间：每半年提供一次网络安全应急演练服务。

交付物：《武汉市第四医院网络安全应急演练记录》、《武汉市第四医院网络安全应急演练总结报告》

4）、网络安全服务人员

交付时间：每日提交日志类，每月巡检结束后三个工作日提交。

交付物：《资产信息库列表》、《漏洞扫描报告》、《配置核查报告》、《新系统上线环境安全评估报告》、《安全检查整改解决报告》、《安全工作日志》、《网络安全状况月报》、《一套网络安全管理体系》、《内外网资产调研台账》

十五、 合同清单

序号	名称	数量	单价（万元）	总价（万元）	备注

1	信息化系统运维服务	1、提供每月一次对全院网络、服务器及存储系统、支撑环境进行性能评估及深度优化巡检服务，形成巡检优化报告； 提供拥有OCP认证的数据库工程师承担全院数据库日常使用保障、运行监控、配置更改、故障排查、数据全量、增量备份服务，并提供每月一次的深度巡检，对配置文件、数据文件、日志文件、备份策略及备份情况进行健康性检查并进行优化，形成巡检优化报告； 2、定期对重要业务虚拟机进行模拟故障恢复，保障备份虚拟机能够正常恢复；以及每年四次数据库还原演练、数据恢复测试，提供全流程的灾难恢复演练操作手册； 3、提供不少于三名高级工程师的应急支撑团队，提供7*24小时技术支持服务，应对突发性、紧急事件的会诊和保障恢复等情况（包含服务器、小型机、网络、存储等系统），以及医院新系统上线、设备迁移变更等情况，提供现场技术支持和技术保障服务； 5、未到设备生命周期末期的继续购买硬件维保及软件升级服务，在质保期内的设备协助院方联系原厂进行维修或更换，过保的设备协助院方进行维修恢复（过保设备的维修费用据实结算）； 6、提供一人/年的5*8小时驻场服务，以及7*24小时的响应服务，负责全院信息资产统计，网络、服务器、存储、虚拟化系统的日常监控、运行维护、故障处理等工作，定期规范检查各硬件设备的运转情况和软件系统运行情况，处理并解决采购人临时的工作安排。	1	77.85	77.85	

2	安全保障运维服务	1、针对医院要过等保测评的业务系统（包括三级系统和外联的二级系统），提供每个业务系统一年一次高级深度渗透测试服务； 2、提供一年一次的蓝队评估服务，通过专业的高级攻防工程师组成蓝队，针对医院的系统、人员、软件、硬件和设备同时执行的多混合、基于对抗性的模拟攻击，以此来发现医院在系统、技术、人员和基础架构中的存在的隐患以及对网络安全状况进行评估； 3、提供不少于三名安全工程师的应急支撑团队，提供7*24小时技术支持服务，当发生重大网络安全事件时现场响应，并协助进行检测与分析、风险抑制、问题根除，协助业务恢复的服务，以及医院现有的安全设备出现故障且无法修复的情况下提供备件备机响应服务； 4、配合开展医院网络安全应急演练服务（一年2次），包括制定应急演练方案设计、搭建演练环境、参与演练、协助编制演练总结； 5、根据医院信息安全管理体系要求，结合医院自身实际情况和需求，每半年进行信息安全管理体系方案修订与增补；根据国家政策相关标准要求，制定网络安全规划方案，建立医院网络安全保障体系以及其它日常安全咨询服务； 6、提供一人/年的5*8小时驻场服务，以及7*24小时的响应服务，负责对全院的安全设备提供定期巡检、预防性维护、配置变更管理、资产清理、处理威胁预警等；一年提供2次资产发现服务；协助处理网络安全紧急事件；协助进行网络安全迎检检查工作；协助进行网络安全宣传；协助进行新上线的重要业务安全评估：协助进行新上线业务进行漏洞扫描、基线配置核查服务；处理并解决采购人临时的工作安排；	1	66	66	提供奇安信原厂服务
3	原厂一年维	HDS G200存储 （4台） 联想flex刀箱+6块刀片服务器(1套) 联想X3850X6服务器(4台) 黑盾流控设备包含一年的URL库，应用特征库及软件固体升级，含一年技术支持（2	1	46.7	46.7	

	保清单	台） 东院+西院准入，盈高 ASM6305（2 台）				
合计			190.55			

以下无合同正文。

甲　　方：武汉市第四医院

单位名称（盖章）：

单位地址：武汉市硚口区汉正街 473 号

授权代理人（签字）：

签约时间：2021 年 12 月 20 日

乙　　方：武汉光谷信息技术股份有限公司

单位名称（盖章）：

地　　址：武汉东湖新技术开发区高新大道 888 号高农生物园总部 A 区 19#楼

授权代理人（签字）：

签约时间：2021 年 12 月 20 日

附件一

信息安全保密承诺函

致：武汉市第四医院

根据国家有关信息安全及信息保密相关法律法规。武汉光谷信息技术股份有限公司（以下简称“乙方”）就武汉市第四医院（以下简称“甲方”）2022年信息系统及安全保障运维服务项目实施及后期系统使用过程中从甲方获取的有关资料和信息的安全保密事项做到以下承诺。

一 保密内容

1. 乙方从甲方获取的资料和信息，一切权利归甲方所有。

2. 乙方不得以任何形式向第三方透露从甲方获取的资料和信息。

3. 乙方保证从甲方获取的资料和信息仅用于与本项目合作有关的用途和目的。

4. 乙方保证对甲方提供的保密信息予以妥善保存，并采取与自身保密信息同等级别的措施和审慎程度进行保密。乙方确保本次项目涉及的所有医院数据必须保留在医院内，没有任何形式外泄。

5. 乙方向其内部提供甲方保密信息的范围应进行严格控制和管理。乙方须向其掌握甲方保密信息的内部人员提示信息的保密性和其应承担的保密义务，并保证上述人员以书面形式同意接受本协议条款的约束。若乙方人员出现岗位调动或离职的情形，乙方有义务立即通知并配合甲方终止其与甲方有关的信息访问权限，收回其所持有的甲方保密资料和涉密介质，并确保该人员在离职后继续履行好保密义务。

6. 若乙方与第三方合并、被第三方兼并或被第三方直接或间接控制，在未经甲方书面授权同意的情况下，乙方不得向该第三方披露任何甲方的保密信息。若出现该情况，乙方应立即将甲方的保密资料归还甲方，或根据甲方的要求予以销毁，不得留存任何资料的备份。

7. 乙方确保在项目合作期间不侵害任何第三方的知识产权或商业秘密。若因本项目发生第三方向甲方主张知识产权的情形，由乙方承担因此产生的一切法律责任。

二 违约和赔偿

1. 乙方应做好内部人员保密管理工作。因乙方在职或离职人员的泄密行为造成的甲方损失，由乙方承担全部责任。

2. 乙方有违反本协议的情形，无论故意与过失都应当立即停止侵害，并在第一时间

采取一切必要措施防止保密信息扩散，尽最大可能消除影响、减少损失，并及时通知甲方。

3. 乙方应承担因违反本协议造成的全部法律责任和对甲方造成的经济、名誉损失。甲方保留向乙方违约行为要求违约赔偿的权利。

三 保密信息的归还

本项目合同终止后，协议所涉及的一切甲方保密信息，无论是书面、电子还是其他具体形式，以及乙方所作的复印件、电子副本均需立即交还甲方或者予以销毁。乙方不允许保留任何形式的资料备份。

四 争议的处理

本协议在履行过程中发生的争议，由双方当事人协商解决，也可由有关部门调解；协商或调解不成的，可考虑提请甲方所在地人民法院裁决。

本承诺书一式两份，甲方乙方各壹份，自加盖乙方公章之日起生效。

承诺人（盖章）：

日　　期：　　年　　月　　日

附件二：外包业务工作考核表

外包业务工作考核表					
类别	考核项目	分值	考核标准	得分	存在问题及整改要求
服务能力	1.维保单位应取准备相应维修工具、应急维修配件。（8分）	20	1.维修工具齐全得4分 2.应急维修配件齐全得4分。		
	2.维保作业人员应进行相关技能培训后上岗。（5分）		维保人员专业技能不能胜任岗位的不得分，满分5分。		
	3.关键人员流失。（2分）		每发生一人次人员流失（变更）扣2分。		
	4.维保期间不得发生重大安全事故。（5分）		未发生人员伤亡重大安全事故得5分，否则不得分。		
服务质量	1.在医院迎接重大检查或重大安全生产保障期间提供运维保障。（6分）	20	未及时提供运维保障服务不得分。		
	2.发生故障或紧急事故时，维保单位应有维修记录或故障维修报告。（14分）		1.未按要求填写记录的，一次扣2分。 2.未如实填写记录或记录填写不全的，一次扣2分。 3.发现无法处理的问题不及时上报信息科管理人员的，一次扣2分。 4.发生重大事故未及时上报管理人员的，一次扣7分。		
服务态度	1.与管理人员和报修人员积极沟通。（5分） 2.维保人员衣着整洁。（5分） 3.值班室干净整洁，不得堆放杂物。（5分） 4.提高满意度，降低投诉率。（5分）	20	1.沟通表达清晰准确，态度得体得5分。 2.未文明着装扣5分。 3.值班室不整洁的扣5分。 4.发生投诉每次扣2分。		
服务效率	在合同约定响应时间内提供运维服务。（20分）	20	发生超期未响应情况每次扣2分。		
服务纪律	严格确保值守、维修的时间响应要求。（20分）	20	1.是否在大型检修前在放置检修护栏，维保后保持现场清洁5分。 2.驻场人员未按正常工作时间到岗，每次扣1分。 3.维保人员电话是否保持畅通5分。		
总分：					
审核人签字：					

附件三

廉洁承诺书

武汉市第四医院：

根据国家、省、市有关规范卫生行业的流通领域行为规范和卫生部“九不准”的规定，本着自我约束规范销售行为的精神，我公司郑重承诺如下：

一、 我公司销售给贵院的产品、保证相关证件齐全，并严格执行省市各项有关政策规定，认真履行合同。

二、 本公司的销售行为按规范严格自律，不以任何理由和方式向贵院的工作人员实行销售提成或给予回扣等违纪行为，若有违反，愿接受贵院中止购销合同和其他一切业务，并承担相应的经济和法律责任。

三、 遵守贵院的有关规定，在与贵院的业务合作中，不直接与使用科室的医务人员进行商业性洽谈，只与院方的业务主管部门进行业务联系，并做到按时、按量供货，以优质的服务保持合作关系。

公司名称（公章）：

法人代表（签章）

年 月 日