第三部分　技术需求书

1. 项目背景

随着北京妇幼保健院（以下简称：北京妇幼）信息化快速发展、医院业务功能不断增加、服务范围加速扩张，当前国内、外的网络安全环境日益复杂，其面临的内外部安全隐患也日益突出。为切实提高北京妇幼信息网络自身信息安全防护能力，当前应按照国家信息安全等级保护制度的相关要求，总结自身信息安全问题，明确自身业务特点与等保二级合规差距和安全建设需求，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等几个方面，提出合理的网络安全运维方案，以进一步推动信息安全责任的落实及信息安全保护工作长效机制的建立，全面保障医疗业务信息化健康发展，使北京妇幼信息网络安全稳定运行。

2. 项目需求清单

序号	项目名称	单位	数量	备注
1	安全巡检服务	次	4	服务期一年
2	应急保障服务	年	1	服务期一年
3	安全策略优化服务	次	1	服务期一年
4	机房运维服务	项	1	服务期一年
5	漏洞扫描服务	次	1	服务期一年

服务设备清单

序号	设备名称	型号	数量	备注
1	互联网防火墙	天融信 TG-A2614	1 台	服务期一年
2	互联网防火墙	天融信 NG-51028	1 台	服务期一年
3	交换机	思科 3750	2 台	服务期一年
4	交换机	DES-1024R	2 台	服务期一年
5	上网行为管理设备	天融信 TI-5228-BJ	1 台	服务期一年
6	机柜	/	4 个	服务期一年
7	服务器原厂主机硬盘	/	1 批次	服务期一年

3. 项目建设详细指标要求

3.1. 网络安全巡检服务

序号	指标项	规格要求
1	服务内容	需利用检测工具和人工检测等多种方式定期对北京妇幼本地信息网络的服务器、网络及安全设备的健康状态进行检测，包括设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作,做好巡检记录，维护记录单，提交巡检报告，确保网络正常。服务内容

		包括： 网络设备巡检：对网络设备的资源使用情况、接口和连接情况进行检查；并重点对安全策略进行检查，及时发现存在的安全隐患或问题，以便及时进行处理。 服务器巡检：对信息系统服务器的 CPU 使用率、内存使用率、硬盘使用率等情况，以及运行进程、后台服务、中间件和数据库运行的安全状态等进行检查，并重点对操作系统、数据库的安全策略进行检查，及时发现存在的安全隐患或问题。 安全设备巡检：对各种安全设备的资源使用情况、接口情况和连接情况等进行检查，重点针对安全策略进行检查，及时发现存在的隐患或问题。 日志分析：针对服务器、安全设备巡检，并从安全设备和重要服务器收集当月日志信息，并对收集到的日志信息进行分析、审查，将日志分析结果以报告和图表等方式撰写审计报告，日志分析：通过对网络设备、服务器系统日志的分析与安全设备日志分析，发现安全漏洞，以便提出相关的安全标准、策略和防护要求。
2	服务方式	应采取检测工具和人工检测实施现场和远程检测相结合的方式
3	服务范围	北京妇幼指定系统涉及资产
4	服务频次	服务期内提供 4 次
5	服务成果	《北京妇幼保健院网络安全巡检报告》

序号	指标项	规格要求

1	服务内容	投标人需确保在第一时间对北京妇幼网络信息系统面临的紧急安全事故进行及时响应。紧急安全事故包括：大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件等。在发生安全事件时按照安全事件的等级进行处理，并在事后进一步分析原因，提供详细的事件响应报告。 投标人同时需辅助医院制定完善的应急预案。应急预案包括（但不限于）不同信息安全事件的应急响应流程、时间及处理方式等。并在北京妇幼本地网络发生安全事件时及时响应，执行应急响应流程，需通过专家级技术支持和快速响应，及时抑制和消除用户网络安全事件，减少损失和负面影响，提高北京妇幼信息网络业务连续性。在“十一”、“五一”、国家重大活动等重要保障时期，指定专人提供现场安全检查服务，对期间网络及重要信息网络安全运行情况进行安全检查，确保北京妇幼网络的安全运行。
2	服务范围	北京妇幼指定系统
3	服务频次	服务期内按需响应
4	服务成果	《北京妇幼应急响应报告》

3.2. 应急保障服务

3.3. 安全策略优化服务

序号	指标项	规格要求
1	服务内容	投标人需针对北京妇幼本地现有安全设备、更新后路由器、交换机等设备策略进行优化，并针对实际环境按照等级保护二级要求进行安全策略加固，重新划分网络安全区域，制定安全访问策略，提升整体网络安全性。

2	服务范围	北京妇幼指定系统
3	服务频次	服务期内提供 1 次
4	服务成果	《北京妇幼安全策略优化报告》

3.4. 机房运维服务

序号	指标项	规格要求
1	服务内容	投标人需针对现有机房老旧设备、配合北京妇幼进行报废处理、硬盘安全存放、报废设备拆除及清洁现有机房环境，对机房所有的设备打标签，包括 4 个机柜、设备和配件等。保证机房相对独立的物理环境安全。并对机房设备及供电系统、UPS 系统、空调系统等设备进行检查，及时发现设备隐患，排除故障。保证机房相对独立的物理环境安全。
2	服务范围	北京妇幼机房
3	服务频次	服务期内提供 1 次
4	服务成果	《北京妇幼机房运维服务报告》

3.5. 漏洞扫描服务

序号	指标项	规格要求
1	服务内容	投标人须通过远程或者现场方式（具体方式由用户依据实际情况确定）使用专业的扫描工具对医院相关系统及涉及资产进行扫描，为安全策略优化提供安全建议。
2	服务范围	北京妇幼机房
3	服务频次	服务期提供 1 次

4	服务成果	《北京妇幼漏洞扫描服务报告》

4. 项目实施要求

项目期限：自合同签订起 1 年。

4.1.服务响应速度

投标人应承诺提供 365×24 小时的热线服务电话和相关通讯方式作为服务接口，委派专人集中受理服务请求，并保证通讯线路畅通。

投标人应承诺按服务响应时间要求提供服务：

7×8 小时内，电话 5 分中内及时响应，电话技术支撑无法解决的，发现故障后立即进行现场响应；

7×8 小时外，电话 15 分钟内响应，电话技术支撑无法解决的，2 小时内到达现场。

投标人应承诺在接到服务需求后，如因自身力量无法完成的，需立即协调原厂技术人员按上述响应速度要求提供服务，所产生费用由服务提供方承担。

4.2.实施团队要求

投标人应为本项目设立不少于 4 人的项目团队，其中应包含 1 名专职项目经理，负责了解采购人需求、制定服务计划、监督服务执行、跟踪并改进服务质量、提交各类服务报告、处理投诉等。项目经理要求具有 5 年（含）以上项目管理经验，需同时具备 CISP 证书、C-CCSK 证书、ITIL 证书、信息系统项目管理师证书、高级工程师职称证书（信息安全专业），至少担任过 3 个同类安全服务项目，合同期内项目经理不得更换。

项目服务团队其他成员具有计算机相关专业教育背景，有 3 年（含）以上安全维护工作经验，熟悉计算机信息安全管理。人员应具备 CISP、CCNA、CCNP、CISP-A 证书之一，团队中需有人具备有效的信息安全等级测评师证书，并能够现场解决用户的安全咨询问题。工作态度认真，责任心强，工作踏实细心，有较强的理解能力和较流畅的语言表达能力和沟通能力。保证网络稳定运行，发生告警后第一时间进行处理，并进行跟踪直到告警消除，主动避免各类安全事件的发生。

4.3.服务网络

除本项目团队人员外，投标人应配备不少于本项目所需的、有相应资质的二线技术支撑技术人员，并提供有效证明。

5. 项目管理要求

5.1. 项目管理工作内容

在本项目建设过程中，投标人应在项目管理领域需要完成的工作主要包括：

（1）对整体项目进度进行控制，保证项目按时提交。

（2）组织协调项目各环节工作，保证项目顺利推进。

（3）制定整体项目目标、分阶段目标，并制定各类目标相应的考核计划，规避各类项目风险保证项目质量。

（4）管理项目团队的组织和人员，为项目提供组织保障。

（5）服从采购人项目组的管理，依从安全整体框架设计和要求，保证北京妇幼服务建设工作。

5.2. 项目管理实施方案要求

针对本项目，投标人需提出项目管理的实施方案和措施：

（1）范围管理措施

投标人应通过需求调研，明确项目的范围，确认工作边界。

（2）进度控制与过程管理措施

投标人应提出对本项目进度控制和过程的管理措施，对进度控制的过程、进度管理的体系、过程管理方式提供详细方案。

（3）质量控制措施

投标人应定义本项目的质量控制活动的组织、质量控制任务和质量职责的划分；为执行质量控制任务提供参考资料和指导；为执行质量控制活动提供标准和约定；为质量控制活动和总结提供工具、技术和方法支持。

（4）风险管理措施

建立风险管理机制，提供风险管理与控制策略。

（5）档案管理措施

投标人应协助采购人完成项目过程中的档案管理工作，明确档案管理职责，采取有效措施对项目后续参建项目形成的档案进行统一管理，保证档案实体和信息的安全。

6. 技术支持与售后服务

投标人应针对医院网络使用与运行需要，提供详细的技术支持与售后服务方案以及服务承诺。对于各类故障必须提供(7×8 小时内，电话 5 分中内及时响应；7×8 小时外，电话 15 分钟内响应。)响应服务，若远程不能解决问题，须派人到现场上门服务，排除故障，并分析故障原因，提出书面故障分析报告及防范措施。