**北京胸科医院信息安全运维项目需求说明**

为了保障医院核心业务系统持续、稳定的运行，确保信息系统安全满足国家相关标准、规范要求，需要按照《北京市卫生局关于进一步加强北京卫生行业信息安全等级保护工作的通知》京卫办[2012]26号文件和等级保护的基本要求，对核心业务系统即HIS系统（三级）开展安全服务工作。

基于HIS系统定级基础上，开展安全巡检、风险评估、安全加固、等保测评等工作，以科学制定信息系统安全保障与持续策略，落实《卫生行业信息安全等级保护工作的指导意见》（卫办发【2011】85号）和《关于进一步加强北京市卫生行业信息安全等级保护工作的通知》（京卫办字[2012]26号）文件要求，建成一个覆盖推进院以HIS系统为核心的高效、有序、可持续发展并满足等级保护三级防护要求的信息安全保障体系，全面保障HIS系统为核心的应用平台安全稳定、持续运行。

具体工作内容:

1. **安全巡查服务**

**服务内容：**

针对日常业务系统的运行情况，厂商应指派专人每月对胸科医院信息系统运行健康状态进行巡查和检测，并将检测结果定期汇报给胸科医院信息部门相关负责人，及时发现并消除日常运行过程中的安全隐患，确保胸科医院相关业务持续运行。

**服务频率：**12次/年

**交付成果：**《安全巡查报告》

1. **杀毒软件维保**

**服务内容：**

厂商需为胸科医院目前所使用的360杀毒软件采购升级服务，保证客户端按时进行病毒库的升级，全面检测已知和未知的各种病毒。

1. **应急响应**

**服务内容：**

全年在出现突发、紧急安全事件时，提供7\*24小时的应急响应服务，协助胸科医院进行有效的应急处理，最大限度地减少信息系统的损失和负面影响。厂商应具备完整的应急体系，应急响应服务应满足：1小时响应，2小时到达用户现场，4小时恢复系统运行的指标。

**服务频率：**6次/年

**交付成果：**《安全应急工单》

1. **风险评估**

**服务内容：**

厂商结合等级保护相关要求对胸科医院的信息系统开展风险评估工作，具体工作内容包括：资产识别、威胁识别、脆弱性识别、安全措施识别、风险分析。

**服务频率：**1次/年

**交付成果：**《风险评估报告》

1. **策略维护**

**服务内容：**

胸科医院系统网络拓扑结构相对复杂，医院的信息系统也将根据实际需要临时调整和增加。因此，每次系统结构的优化调整，都将会影响信息安全整体目标的调整。厂商需要辅助优化信息系统结构，提出合理的优化加固方案，调整软硬件策略逐步趋于合理，从整体结构上提高抗风险能力。

厂商需根据需求及信息安全最新态势，制定安全设备的安全防护策略，定期进行维护，确保安全设备能够抵御最新的安全威胁。

**服务频率：**1次/年

1. **安全加固**

**服务内容：**

厂商需根据国家信息安全等级保护相关要求，结合胸科医院实际情况在服务期内对网络设备、安全设备和服务器系统（操作系统、数据库、中间件）进行安全策略加强、调优等，以加强网络、系统和设备抵御攻击和威胁的能力，整体提高胸科医院信息系统安全防护水平。

**服务频率：**1次/年

**交付成果：**《安全加固报告》

1. **等保咨询**

**服务内容：**

厂商需为胸科医院设计信息系统功能结构、技术路线方案、应用平台方案、数据库方案、系统安全方案、系统集成方案、系统维护和扩展方案、项目周期、项目收益及风险分析、项目实施方案等提供咨询和帮助；并为胸科医院信息化产品选型提供模型、测试方案等。

**服务频率：**1年

1. 等级保护管理体系修订

**服务内容：**

厂商需参照胸科医院原有信息安全管理制度，结合国家关于等级保护的要求，对机房管理、资产管理、系统上线、系统变更、口令管理、网络安全、审计监控和数据备份等安全管理制度进行适应性修订；并组织运维人员对制度进行论证，确保制度贴合医院实际，具有可操作性。

**服务频率：**1次/年

**交付成果：**《等级保护管理制度》

1. **辅助测评**

**服务内容：**

厂商需针对胸科医院的重要信息系统提供现场测评辅助，在测评机构对重要信息系统测评期间，需派驻专业工程师提供全流程的测评辅助服务，配合测评机构完成重要信息系统的现场测评工作。针对测评机构测评过程中发现的问题，从技术优化和管理制度完善两个方面制定安全整改与优化方案，在得到医院的认可后，协助医院完成网络安全、主机安全、数据库安全等问题整改。提供复测期间的辅助服务，针对测评机构在复测期间的测评工作进行配合，并针对复测期间发现的问题及时进行整改，以使重要信息系统达到安全等级测评要求。

**服务频率：**1次/年

1. **等保测评**

**服务内容：**

聘请有专业资质的测评机构对胸科医院信息系统进行测评工作， 并出具相关报告。包括

信息系统安全体系架构合理性分析：对系统安全体系架构的正确性、合理性进行分析；

渗透性测试：对网络与信息系统存在的漏洞和隐患实施本地或远程渗透性检测与验证；

脆弱性评估：从物理层、网络层、系统层、应用层、安全管理层五个方面识别系统的安全隐患；

安全配置检测：对网络、主机、数据库、应用的安全性和稳定性进行检测，分析安全配置中存在的安全隐患。。

**服务频率：**1次/年

**提交成果：**《信息安全等级保护测评报告》