****第一节总则****

　　1、为加强医院信息技术外包服务的安全管理,保证医院信息系统运行环境的稳定,特制定本制度。

　　2、本制度所称信息技术外包服务,是指医院以签订合同的方式,委托承担信息技术服务且非本医院所属的专业机构提供的信息技术服务,主要包括信息技术咨询服务、运行维护服务、技术培训及其它相关信息化建设服务等。

　　3、安全管理是以安全为目的,进行有关安全工作的方针、决策、计划、组织、指挥、协调、控制等职能,合理有效地使用人力、财力、物力、时间和信息,为达到预定的安全防范而进行的各种活动的总和,称为安全管理。

　　4、外包服务安全管理遵循关于安全的所有商业准则及适当的外部法律、法规。

****第二节外包服务范围****

　　5、外包服务包括信息技术咨询服务、运行维护服务、技术培训等。

　　6、咨询服务:

　　6.1根据医院的信息化建设总体部署,协助医院制定切实可行的技术实施方案。

　　6.2对医院现有的信息技术基础架构、设备运行状态和应用情况进行诊断和评估,提出合理化的解决方案。

　　6.3根据医院的实际情况提出备份方案和应急方案。

　　6.4其它信息技术咨询服务。

　　7、运行维护服务:

　　7.1软硬件设备安装、升级服务。

　　7.2硬件设备的维修和保养。

　　7.3根据医院业务变化,提供应用系统功能性的需求解决方案及执行服务。

　　7.4系统定期巡检和整体性能评估。

　　7.5日常业务数据问题的处理服务。

　　7.6其它运行维护服务。

　　8、技术培训:根据医院的实际情况,提供相关的技术培训。

****第三节外包服务安全管理****

　　9、外包服务安全管理应按照“安全第一、预防为主”的原则,采取科学有效的安全管理措施,应用确保信息安全的技术手段,建立权责明确、覆盖信息化全过程的岗位责任制,对信息化全过程实行严格监督和管理,确保信息安全。

　　10、成立由分管领导同志信息化外包管理组织,明确信息化管理的部门、人员及其职责。

　　11、建立信息建设安全保密制度,与外包服务方签订安全保密协议或合同,明确符合安全管理及其它相关制度的要求。并对服务人员进行安全保密教育。

　　12、制定信息化加工过程管理、信息化成果验收与交接、存储介质管理等操作规程或规章制度。

　　13、外包服务方的人员素质、技术与管理水平能够满足拟承担项目的要求,进行相应的安全资质管理。

　　14、信息中心配备专人负责安全保密工作,负责日常信息安全监督、检查、指导工作。对服务方提供的服务进行安全性监督与评估,采取安全措施对访问实施控制,出现问题应遵照合同规定及时处理和报告,确保其提供的服务符合医院的内部控制要求。

　　15、对外包服务的业务应用系统运行的安全状况应定期进行评估,当出现重大安全问题或隐患时应进行重新评估,提出改进意见,直至停止外包服务。

　　16、使用外包服务方设备的,对其进行必要的安全检查。

　　17、在重要安全区域,对外部服务方的每次访问进行风险控制;必要时应外部服务方的访问进行限制。

****第四节附则****

　　18、本制度由信息中心负责解释。

　　19、本制度自发布之日起生效执行。