安全准入项目说明

为提高我院的工作效率，我院已陆续完成HIS系统、电子病历系统、LIS、PACS等医院信息系统的建设工作。为响应国家、行业主管们有关信息安全政策法规要求，按照卫生行业等级保护工作指导意见，我院已将HIS系统定级为等级保护三级系统。

随着《网络安全法》的发布施行，国家网络安全保障制度和标准体系也在逐步完善，2018年6月，由公安部牵头制定的《网络安全等级保护条例》发布征求意见稿，与此同时，等级保护核心系列标准也基本修订完成，此外，针对关键信息基础设施的相关制度和标准也在加紧制定中。

2019年12月1日起，《信息安全技术 网络安全等级保护基本要求》（以下简称“等保2.0”）正式实施，标志等保工作进入到2.0阶段，为进一步落实等保2.0要求，完善网络安全体系、提升网络安全服务能力、保障业务系统正常稳定运行，需要对我院对网络安全准入系统进行建设。

本次准入项目需要满足如下要求：

满足《网络安全等级保护基本要求》

应能够对非授权设备私自联到内部网络的行为进行限制或检查

应能够对内部用户非授权联到外部网络的行为进行限制或检查

应关闭不需要的系统服务、默认共享和高危端口

应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理

对内网所涉及的终端，部署准入客户端

开启相应的安全防护策略，禁止未安装准入的用户接入到医院网络

对U盘、高危端口进行封禁；

对终端的安全漏洞进行扫描，集中进行补丁下发；

对终端所需的软件进行集中下发；

对终端进行安全管控，开启程序白名单

通过准入系统对安全终端进行集中管控；

终端出现故障，可迅速定位，通过远程的方式快速解决问题；

通过对U盘的封禁，减少因U盘乱插造成的病毒传播；

通过准入系统的部署，及时发现非法外联的接入，并进行阻断，减少因非法接入医院网络所造成的攻击。

开启程序白名单，对终端用户可开启的软件进行管控。

发现未知的终端设备，进行安全管理

授权设备数量需大于1000个终端