服务需求一览表

序号	设备名称	技术参数	数量	备注
1	智慧校园网络信息安全运维服务（一年）	1、安全评估服务 使用各种安全检查工具（包括但不限于漏洞扫描等）和人工测试手段，通过互联网方式或内网接入方式，对指定的服务器、核心网络设备进行漏洞检查和风险评估服务。安全评估完成后将详细过程和细节以书面报告的形式提交给学校，内容包括可以被利用的各种安全风险和安全隐患等。每年不少于 3 次。 2、渗透测试服务 完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节，并对发现的问题给出解决建议。每年不少于 3 个系统。 3、安全加固服务 协助学校或第三方开发厂商对发现的漏洞和脆弱性进行加固整改，降低安全隐患，提高系统的抗风险能力；并且提供加固后的验证服务。每年不少于 3 次。 4、新系统上线检查服务 为了消除新上线系统可能存在的安全漏洞或安全隐患，同时满足的安全管理要求，对自主开发、合作开发或外部采购的应用系统执行上线前安全检查服务。从网络环境、系统环境、数据库、Web 应用等层面对新上线系统或重大改版系统进行综合的风险分析，并针对存在的安全弱点提供改进建议。每年不多于 3 个系统（根据学校具体情况确定）。 5、安全通告服务 组织安全专家不断自主挖掘漏洞、关注安全技术的发展、安全漏洞的发布、恶意病毒传播等信息，并根据的信息资产情况定期和在需要的时候（重大安全事件发生时随时通告）提供安全信息通告服务，提醒学校及时采取防御性措施。每年不少于 3 次。 6、应急响应服务 当信息系统发生突发的安全事件时，安全专家应在第一时间提供应急响应服务，协助学校对安全事件进行分析、处理，并提供安全事件应急响应报告和	1	

		安全改进建议报告。每年不多于 5 次（根据学校具体情况确定）。 7、网站安全监测服务 不少于 5 个域名一年的网站安全监测服务，监测项目包括网站漏洞扫描、挂马监测、可用性监测、页面篡改监测、域名解析监测、敏感内容监测。通过网站安全监测平台对网站进行自动化监测，通过邮件进行及时报警，每周、每月发送监测报告。 8、重要时期安全保障服务 根据学校需要在重大保障期间（如两会、国庆等）进行现场职守服务，每年不多于 25 天（根据学校具体情况确定）。 9、应急演练服务 制定应急演练方案，并依据演练方案进行应急演练，熟悉应急流程，明晰各相关人员在发生应急事件时的相应方式及流程。每年不少于 1 次。 10、安全巡检服务 每一季度对服务范围内的设备进行巡检，并出具巡检报告。 11、安全培训服务 根据学校要求，对师生进行的安全意识培训，对技术人员进行安全技术的演示及相应的指导性培训工作（不超过 24 课时）		
其他补充内容： 1、实施地点：学校指定地点； 2、服务期：自签订合同起一年内； 3、验收标准：中标方保证其服务质量及技术达到国家现行技术标准和合同约定标准或投标文件承诺标准。针对项目要求中的技术要求进行逐一验证，满足服务要求中的各项指标，并提供相关的技术文档、实施文档及学校要求的项目验收报告； 4、其他售后服务等：中标方应对服务响应时间、解决故障的所需要的时间做出承诺。				