福建高校思政工作网信息系统等级保护（二级）咨询与评测服务项目技术和服务要求

通过等级保护咨询服务实施，最终完成服务范围内的信息系统通过第二级网络安全等级保护测评，测评结果为“基本符合”及以上。 1、定级咨询

参照国家和地方对网络安全等级保护定级的有关要求，对网络安全开展摸底调查工作，掌握信息系统的基本情况，了解信息系统的业务类型、应用或服务范围、用户数量、系统结构、部署方式、安全策略、内控制度等信息，撰写网络安全定级报告，明确网络安全的边界和安全保护等级，说明定级的方法和理由，收集整理网络安全定级所需的资料和文档。同时协助采购人组织并完成等级保护专家定级评审工作。

 2、等级保护备案

按照《等级保护基本要求》完成系统等级保护备案工作，并取得公安机关出具的等级保护相关备案证明。

3、资产分析服务

3.1 资产调查：调查和统计信息资产，包括但不限于物理环境、网络设备、主机、应用软件、业务系统、数据、人员、标准流程等，明确其现有状况、配置情况和管理情况，并对所有信息资产按照一定标准进行资产赋值，绘制各业务系统的数据流图。正式开展调查时调查内容需经采购人审核后实施。 3.2 网络拓扑调查：包括对所有网络的拓扑结构进行调查，并按统一标准绘制成图。 3.3安全系统调查：包括但不限于明确现有安全设备的部署情况和使用情况，编制安全区域图。

4、 差距评估服务

4.1根据网络安全等级保护基本要求，开展物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理和安全运维管理现状评估，差距评估应当覆盖等级保护技术要求。

 4.2根据等级保护的相关标准和要求，分析主机安全、应用安全和数据安全面临的威胁，评估现有系统的存在的弱点，明确现有网络面临的安全风险和隐患。

4.3应用系统风险评估：对业务系统存在的脆弱点进行综合评估，结合系统情况对漏洞的风险等级进行赋值，输出《风险评估报告》。

4.4管理制度梳理与建设 （1）管理制度梳理：从信息安全方针、管理体系、安全管理机构的设立、人员管理、重要区域访问控制、网络安全建设管理、产品采购、系统运维管理、恶意代码、备份恢复策略、应急响应等深入评估采购人网络安全管理制度与等级保护标准差距。 （2）管理制度建设：结合采购人网络安全的实际情况，协助采购人建设安全管理制度，主要包括但不限于信息安全工作职责，信息安全监督、检查机制；辅助用户编写方针、制度、各类记录表格模板在内的安全管理制度等。管理制度包括但不限于：《网络安全策略管理》、《安全制度制订流程规定》、《操作系统维护规程》、《数据库系统维护规程》、《网络安全培训管理》、《安全管理日常维护细则》、《安全审计管理制度》、《第三方人员管理制度》、《防病毒紧急响应流程》、《软件开发环境使用管理要求》、《系统交付管理规范》、《安全事件报告和处置管理规范》、《网络安全应急处理体系》、《人员安全管理规范》、《网络全运维管理规范》等。

 5、安全规划

投标人需根据差距评估结果，结合国家相关法律法规要求，在充分考虑信息系统状况下进行安全域设计，分析安全需求得出安全控制措施，并对安全控制的相关性、紧迫性、可实施性、难易程度和预期效果等进行分析，对采购人未来几年信息安全工作进行规划，提出可行的安全解决方案和安全规划。 6、安全整改 投标人需根据差距评估结果和安全规划，结合等级保护要求，对于安全评估后在技术和管理中发现的安全漏洞和安全脆弱性情况以及与等级保护要求之间的差距，提出可行的安全整改方案，以达到等级保护基本要求。

7、二级等保测评服务

（1）投标人必须确保信息系统安全等级保护工作能顺利完成，并承诺可一次性通过福建省网络与信息安全测评中心测评，如果未一次性通测评，由此产生的费用及相关损失全部由中标人承担，需提供书面承诺。