**上海海洋大学信息系统安全等级保护测评项目**

**服务需求**

# 一、项目背景

近些年，互联网上恶意威胁攻击手段不断出现，并被肆意传播和使用，给高校的信息化应用带来了严重影响。对此，教育部办公厅于2009年11月11日面向全国各级教育管理机构正式下发了“关于开展信息系统安全等级保护工作的通知”（教办厅函[2009]80号），决定在全国教育系统全面开展信息系统安全等级保护工作，“通知”指出：“要重点保护基础信息网络和关系教育网络安全、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

上海海洋大学开展信息系统等级保护测评是为贯彻落实上海市及教育部关于信息系统安全等级保护有关政策规定和技术标准规范，尽快提升上海海洋大学信息安全防护能力、进一步加强安全防护力度，保障教学信息系统安全稳定运行；在遵循公安部关于信息系统等级保护的相关要求下，结合自身的网络及业务应用现状进行信息系统等级保护建设，构建等级化的信息系统安全保障体系架构，形成一个策略、组织、技术和运维相结合的信息安全保障体系，并在系统运维中不断发现和解决问题，建立信息系统安全长久机制，以此来保障教学信息化的顺利健康发展。

# 二、项目服务范围

本次等级测评的对象为以下信息系统：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 系统等级 | 备注 |
| 1 | 上海海洋大学门户网站 | 二级 | 复测 |
| 2 | 上海海洋大学教务系统 | 二级 | 复测 |
| 3 | 上海海洋大学人才招聘网 | 二级 | 初测，需备案 |

本项目由信息安全测评授权机构（列入“中国信息安全等级保护网”全国等级保护测评机构推荐目录）对上海海洋大学的3个重要信息系统进行安全测评工作，按照国家等级保护的要求依据上海海洋大学信息系统实际情况进行安全测评相关工作，满足安全需求。

本次网络安全等级保护测评是通过对学校3个重要信息系统在安全技术层面和管理层面进行安全测评，包含初测和复测，加强对敏感数据的隐私保护以逐渐完成对业务服务及关键数据的安全保护，降低因信息系统引发的安全事件带来影响及损失，保障学校信息系统的各项业务应用以及业务数据的安全可靠。

# 三、安全服务需求清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **技术要求** | **数量** |
| 1 | 等保测评工作 | 协助校方在2020年12月31日前完成并通过三个系统的等保测评，包括但不限于确定测评范围、现状调研、安排测评机构、单元测评、整体测评等各项等保测评所需工作。 | 1 |
| 2 | 安全方案设计 | 根据等保要求，对现状进行调研、分析，相应的差距分析，以及建立安全风险评估模型。 | 1 |
| 3 | 信息安全风险评估 | 对本项目设计的三个系统进行风险评估。分析信息系统可能面临的威胁，当前存在的弱点，以及弱点被袭击或带来破坏的可能性及影响，以此为基础对当前信息系统的安全风险进行分析和定义。 | 1 |
| 4 | 安全整改服务（管理+技术） | 根据等级保护相关要求，协助进行安全加固服务（包括网络安全加固、主机系统安全加固、安全设备加固优化）；建立并完善基于等级保护要求下符合单位信息系统现状和的信息安全管理体系。 | 1 |
| 5 | 1年安全漏扫服务 | 提供1年（合同签订之日起，每月1次）全网安全评估漏扫服务。 | 1 |

# 四、实施原则

本项目按照以下原则和标准规范进行实施：

（一）安全保密原则

在为上海海洋大学提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

（二）最小影响原则

在为上海海洋大学开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，应对风险进行说明。

（三）规范性原则

在为上海海洋大学开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

（四）可控性原则

在为上海海洋大学开展的安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

（五）质量保障原则

在为上海海洋大学开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

（六）标准规范

* GB\_T 22239-2019《网络安全等级保护基本要求》
* GA-T 1389-2017 《信息安全技术网络安全等级保护定级指南》
* GB-T 22239-2019 《信息安全技术网络安全等级保护基本要求》
* GB-T 22240-2018 《信息安全技术网络安全等级保护定级指南》-试行稿
* GB-T 25058-2010 《信息安全技术信息系统安全等级保护实施指南》
* GB-T 25070-2019 《信息安全技术网络安全等级保护安全设计技术要求》
* GB-T 28448-2019 《信息安全技术网络安全等级保护测评要求》
* GB-T 28449-2018 《信息安全技术网络安全等级保护测评过程指南》
* GB-T 36627-2018 《信息安全技术网络安全等级保护测试评估技术指南》

# 五、技术要求

本项目安全服务技术要求至少包括以下内容：

* 1. 定级备案服务

根据上海海洋大学的要求，对上海海洋大学人才招聘网信息系统进行定级备案服务。服务内容包括针对学校未定级的信息系统进行调研，按照《信息安全技术信息安全等级保护定级指南》确定安全等级保护级别，了解信息系统的服务对象、服务范围、基本的功能用途，依赖的软硬件资产等，确定信息系统业务信息的安全级别，编写《信息安全等级保护定级报告》和《信息安全等级保护备案表》，并协助上海海洋大学向公安机关完成备案工作。

服务频次：1次。

* 1. 等级保护测评服务

（1）现状调研

针对信息系统网络安全等级测评涉及的资产进行现状调研。

（2）现场协助测评

技术工程师进行现场测评准备、现场测评协助和结果记录、结果确认和资料归还等内容，顺利完成现场测评工作。

（3）安排测评机构

安排具备相应网络安全等级测评资质的机构对上海海洋大学指定信息系统进行安全等级测评，使本项目涵盖的3个信息系统顺利通过安全测评。所选择的测评机构须对网络安全等级保护测评工作具有丰富经验。

（4）单元测评

针对3个二级系统主要从等保2.0的安全通用要求中，安全技术包含的4个方面和安全管理包含的4个方面展开单元测评工作。

安全通用要求中的技术要求，主要包括物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复，主要包括以下方面的内容：

* 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

安全通用要求中的管理要求，主要包括安全管理机构、安全管理制度、安全人员管理、系统建设管理、系统运维管理，主要包括以下方面的内容：

* 安全策略和管理制度
* 安全管理机构和人员
* 安全建设管理
* 安全运维管理

（5）整体测评

针对本项目涵盖的3个二级信息系统进行整体测评，主要包括安全控制间安全测评、层面间安全测评、区域间安全测评、系统结构安全测评。

测评服务方式：包括访谈、调研检查、测试、风险分析等方式进行，同时说明测评服务流程。

安全测评工作频次：1次。

* 1. 编写安全整改方案

根据安全现状调研结果，对上海海洋大学门户网站、上海海洋大学教务系统和上海海洋大学人才招聘网的信息系统安全现状提出成熟的信息安全风险分析模型，对信息系统当前的信息安全风险进行定量分析。在安全技术、安全管理等方面是否符合已确定的安全等级的要求；对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，并在系统整改后进行复测确认，以确保整改措施符合相应安全等级的基本要求。。

* 1. 安全加固服务

根据信息系统检测结果和安全整改加固方案，进行安全加固实施。在不影响系统当前业务开展的前提下，对上海海洋大学门户网站、上海海洋大学教务系统和上海海洋大学人才招聘网信息系统涉及的操作系统、网络设备、安全设备等安全状况及安全配置策略进行加强，及时消除因安全漏洞被恶意攻击者利用从而引发的风险。系统加固服务包含网络结构调整、系统设备脆弱性加固、加固效果跟踪评价三部分工作，具体内容如下：：

* 网络结构优化调整。
* 机房所有主机系统（含虚拟机）：检查主机系统的补丁管理、账号及口令策略、网络与服务、文件系统、日志审核、防火墙策略、系统钩子、rookit、安全性增强。
* 机房所有数据库系统：检查数据库系统的补丁管理、账号及口令策略、传输加密、文件系统、日志审核。
* 机房主要网络设备: 检查网络设备（交换机、路由器、防火墙等）的补丁管理、账号及口令策略、访问控制、网络与服务、日志审核。
* 机房安全设备: 安全设备是否配置最优，实现其最优功能和性能，保证网络系统的正常运行、是否存在漏洞或后门、自身的保护机制是否实现、检查安全设备的补丁管理、账号及口令策略、访问控制、网络与服务、日志审核。
* 协助测评：在整体整改完毕后，确认整改情况并汇总形成阶段报告，同时协助上海海洋大学配合第三方测评单位开展测评。

信息系统安全评估漏扫服务须由专业安全评估系统完成，漏扫过程需遵照OWASP和NIST等国际专业标准。

* 1. 安全管理制度建设

按照国家有关规定，依据《信息安全等级保护基本要求》，参照《中华人民共和国网络安全法》、《信息系统安全管理要求》、ISO27000等标准规范要求，检查并优化用户方信息安全管理组织体系、规范、相关制度。

检查完善信息安全组织体系，明确领导机构和责任部门，落实规范和相关制度。检查完善岗位和人员管理制度，根据职责分工，分别设置安全管理机构和岗位，制订每个岗位的职责与任务，落实安全管理责任制。

根据安全管理需求，检查优化以下内容：确定安全管理目标和安全策略，针对信息系统的各类管理活动，制定人员安全管理制度、系统建设管理制度、系统运维管理制度、定期检查制度等，规范安全管理人员或操作人员的操作规程等，初步建成完善的适合上海海洋大学的安全管理体系。

# 六、实施要求

6.1 工期要求

项目实施团队在具备安全服务实施条件后，立即开展实施信息系统等级保护测评项目，并在2020年12月31日前完成信息安全等级测评项目实施及项目验收工作。

6.2 实施团队要求

 项目实施团队须为本项目组建稳定的、专业的、独立的项目团队，专门负责本项目服务实施工作，进行相关的项目管控和随时调整项目实施方向。针对本项目成立专门的项目组，确保人力、物力的投入，项目组成员必须稳定，项目实施团队成员在项目终验前如果人员退出或更换，需要征得用户方同意。

根据类似项目实施经验，项目经理需具备丰富的项目管理经验，才能有效保障项目实施顺利且保质保量开展，为此项目经理需至少具有5年以上安全集成或安全服务项目实施经验，具有信息安全保障人员认证证书(CISAW)，并出具相关安全集成或安全服务项目实施经验的经历说明和个人简历。

6.3 验收要求

项目实施团队需提交的验收文件资料主要包括:

（1）《上海海洋大学信息安全等级保护备案表》。

（2）《上海海洋大学XXX系统信息安全风险评估报告》。

（3）《上海海洋大学XXX系统信息安全加固报告》。

（4）《上海海洋大学XXX系统网络安全等级保护测评报告》。

6.4 项目管理要求

项目实施团队要求给出切实可行的项目实施方案，方案中要包含风险管理、进度管理、变更管理、沟通管理、文档管理、质量管理、技术保障措施、组织保障措施等内容。

在项目实施的全过程中，项目实施团队接受并配合对项目进度、质量进行的监督控制，定期向用户方提交项目进展情况报告。

6.5 保密要求

项目实施团队要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从招标方的管理，严格遵守招标方的保密规定和工作制度，并承担相应的保密责任。

所有参与本项目的服务人员自觉接受招标方的安全保密监督和管理，如违反安全保密条款，招标方将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还将依法承担相应的民事责任。

6.6 技术支持及售后服务要求

项目实施团队应针对本项目提供详细的技术支持及售后服务方案，方案包括完善的技术支持体系、服务响应流程、响应时间、服务热线、服务保障措施、应急处置措施等内容。

在项目实施期间，项目实施团队需成立专门技术队伍，对项目实施期间涉及的信息系统安全技术问题进行解答，提供7x24小时热线电话服务响应，对服务期间发生的问题在1小时内给予响应，若电话不能解决需2小时到现场进行分析处理。