**项目名称：上海海洋大学电子邮件系统等级保护咨询测评服务项目**

**工作内容**

**一、安全方案设计**

1. 编制《上海海洋大学电子邮件系统等级保护信息安全项目技术方案》，提供全面技术解决方案；
2. 与上海海洋大学确定项目质量控制的关键性节点。

**二、提供全面信息安全服务**

1. 信息安全风险评估：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；
2. 信息安全制度检查与优化：建立并完善信息安全管理体系（含信息安全管理机构、信息安全管理制度、应急体系建设与演练等内容），查找现有信息安全管理制度与等级保护要求之间的差距，建立基于等保要求下，符合我单位信息系统现状的信息安全管理体系；
3. 安全加固服务：根据安全整改加固方案，对上海海洋大学电子邮件系统进行安全加固服务（包括主机安全加固、网络设备安全加固服务、安全设备安全加固优化服务、管理制度完善、协助测评）；
4. 定级备案工作：协助校方完成定级备案工作；
5. 提供相关的安全技术培训；
6. **等级保护测评**

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）对上海海洋大学电子邮件系统系统进行正式测评，并通过测评。

**安全服务需求清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **技术要求** | **数量** |
| 1 | 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，以及安全整改方案 | 1 |
| 2 | 信息安全风险评估 | 对电子邮件系统进行风险评估 | 1 |
| 3 | 安全整改服务（管理+技术） | 根据等级保护相关要求，进行安全加固服务（包括主机安全加固、网络设备安全加固服务、安全设备安全加固优化服务、管理制度完善、协助测评）；建立并完善信息安全管理体系； | 1 |
| 4 | 定级备案工作 | 协助校方完成定级备案工作； | 1 |
| 5 | 等级保护测评 | 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）对上海海洋大学电子邮件系统进行正式测评，并通过测评。 | 1 |
| 6 | 人员培训 | 对人员进行安全培训，提升人员安全意识、安全技能 | 1 |

**安全服务要求**

项目安全服务要求至少包括以下内容：

1. 编写安全整改方案

上海海洋大学电子邮件系统的安全现状提出成熟的信息安全风险分析模型，根据安全现状调研结果，对上海海洋大学电子邮件系统的信息安全风险进行定量分析。同时根据等保要求，对上海海洋大学电子邮件系统进行差距分析，并据此完成安全整改方案。

1. 安全加固服务

根据安全整改加固方案，对上海海洋大学电子邮件系统进行安全加固服务（包括主机安全加固、网络设备安全加固服务、安全设备安全加固优化服务、管理制度完善、协助测评），范围如下：

* 划分电子邮件系统网络安全区域
* 电子邮件系统主机系统（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；
* 电子邮件系统数据库系统：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。
* 主要网络设备: 检查网络设备的补丁管理、账号及口令策略、访问控制、网络与服务、日志审核。
* 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，并取得通过报告。
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《信息系统安全管理要求》、ISO27000等标准规范要求，建立用户方信息安全管理组织体系、规范、相关制度。

建立信息安全组织体系，明确领导机构和责任部门，落实规范和相关制度。建立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，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。

**安全培训要求**

投标方应为用户方信息化技术人员提供信息安全相关专业技术知识培训，提供信息化定制培训课程。

培训课程应包括但不限于以下内容：

* 安全基础知识，加密技术、防火墙技术等网络安全基础
* 安全防范手段简介及技术体系建立，为购置、开发、测试、实施信息系统的实践符合组织的战略和目标提供保证；
* 安全策略概念及制定，为组织的安全政策、标准、程序和控制确保信息资产的保密性、完整性和可用性提供保证
* 安全风险评估操作培训，帮助组织保护和控制信息系统；不断完善并适用于系统开发过程，系统生命周期，应用控制，变更控制，以及用于确保数据和应用程序完整性。

投标人应根据上述要求详细制定培训方案，培训方案应包括培训目的、培训时间安排、人数、次数、培训课程大纲、培训师资情况、培训组织方式等。