**采购需求**

**一、项目概况及总体要求**

**项目概况：**为深入贯彻落实习近平总书记对网络安全工作重要指示精神，提升我校网络安全防范能力，有效保障各类业务系统安全、稳定运行，有效抵御内、外部的各类网络攻击，提前发现学校存在的网络安全问题和薄弱环节，及时进行网络安全整改和加固。我校拟购买专业公司的网络安全服务，通过驻场人员服务和安全专家团队支撑，给我校网络安全工作输入专业的安全管理及安全技术经验，引入网络安全运营团队的能力以及网络安全的情报资源，解决我校网络安全专业人员不足、安全情报不及时等问题。

**总体要求：**投标人要针对我校提出的网络安全服务的需求制定全面、具体的方案，提前确定项目组成员，严格把控项目执行过程。我校对安全服务的团队要求、项目过程控制和服务质量考核要求如下所示：

**（1）团队要求**

为了保证服务质量，项目团队成员必须为从事网络及信息安全服务的专业技术人员，必须是投标投标人本单位员工（提供相关人员信息和相关证书复印件并加盖公章），并提供项目组成员名单及技术分工配置单（如所学专业、研究方向、擅长领域等）。人员一经确认，不得随意变更；

**项目组成员不少于3人**（含项目经理1人，驻场技术人员1人）；

**以上所有成员均需提供近3个月以来任意1个月的社保缴纳证明。**

**（2）项目过程控制要求**

　　项目前期：制定全面、具体的服务方案。

　　项目进行：阶段性服务工作完成后需要输出相应的报表、报告等材料。

　　项目结束：编制总结报告，纸质文档交接，电子文档集中销毁。

**（3）服务质量考核**

为评价中标方提供的服务质量，每季度对中标人的安全服务进行考核评分（百分制），年度考核评分为每年四个季度考核的平均分。详细考核机制如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **考核** | **考核项目** | **分值** | **评价描述** | **评分** |
| 工作考核  90分 | 任务完成效率 | 40 | 未充分规划、在规定时间内不能完成任务 | 每次扣5分 |
| 任务完成质量 | 50 | 出现质量异常（投诉、失误、返工） | 每次扣3分 |
| 出现严重质量异常（投诉、失误、返工） | 每次扣6分 |
| 出现因安全服务导致的宕机超过4小时 | 每次扣10分 |
| 响应需求被动，消极处理问题 | 每次扣5分 |
| 人员考核  10分 | 服务质量 | 10 | 不注重沟通，遇到问题以强硬或回避的态度来应对 | 每次扣2分 |
| 服务态度差，甲方收到投诉 | 每次扣5分 |

**考核说明：**

1.考核初始赋值 100分。考核表格包括但不限于以上内容，在实际运作中不断完善。每个考核项目扣分项最多将该项分值扣至0分。

2.每季度考核分数在60到80分之间，将要求中标方对安全服务团队责任人进行谈话，并责令整改。每季度考核分数≦60分，中标方须更换安全服务实施人员，更换人员须符合安全服务人员要求。如无法更换符合要求的安全服务人员，甲方将终止合同，并拒付剩余合同款项。

3.年度评分将作为考核中标方服务质量的依据，作为下一次安全服务招标对中标方评价的重要参考依据。

**二、服务内容**

服务内容包括（不限于）：资产梳理、安全设备巡检、漏洞扫描、新系统上线检测、渗透测试、安全预警、重要时期保障、应急响应、应急演练、安全培训、网络安全宣传周宣传教育、安全咨询与策略优化、安全威胁专项检查等相关工作，主要内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **详细内容** | **服务频次** |
| 1 | 资产梳理、设备巡检 | 1.对校方无限制数量IT资产通过内、外网进行资产情报的搜集，帮助用户发现自己的未知资产，尤其是双非系统（网站），建立IT资产台账（记录其IP地址、操作系统、中间件、数据库版本等信息，并标识业务系统作用和关联系统）。  　　2.安全设备健康度巡检和威胁日志巡检、安全设备告警信息分析、WEB应用分析、DNS行为分析、异常登录分析、邮件分析等。  　　3.安全事件处置：对发现或者发生的安全威胁、事件进行分析、处置、协助校方进行全面整改。 | **服务周期：**项目周期同步  **工作时间：**工作日（8：00至18：00），网络威胁高发时期、重点时期等情况服从学校安排  **交付物**：文字形式的工作日报、周报、阶段性总结等，协助学校做好相关网络安全文件的编制工作 |
| 2 | 漏洞扫描 | 1.针对校方指定网站和信息系统进行全方位多维度自动化的漏洞扫描，通过漏洞扫描工具结合人工确认的方式从内网和外网两个角度发现安全风险、漏洞和威胁。  　　2.给出全面的安全评估报告，对可能存在的误报进行验证，详细说明存在的安全风险，对确认存在的安全风险提供对应的修复建议，并协助校方进行风险修复。一周内提供安全评估报告，紧急情况需3天内提供报告。报告包含原因分析、解决方案以及校方要求的其他内容。 | **服务范围:**服务期内学校提供的所有网站、业务系统（含复测)  **服务频率:**按实际需求  **交付物:**漏洞扫描报告和修复工作 |
| 3 | 新系统上线检测 | 系统上线前安全检测服务主要是针对校方新上线的系统进行安全检测，确保系统在没有中危及以上安全隐患，才允许上线正式运行。系统上线前安全检测方式主要包括：漏洞扫描（内外网结合）、渗透测试。出具详细的安全评估报告，并配合对新系统相关的安全整改与复核。 | **服务频率：**根据学校要求响应  **交付物：**安全评估报告、安全整改与复核 |
| 4 | 渗透测试 | 1. 以模拟黑客入侵的方式对目标系统进行模拟入侵测试，最大限度挖掘注入漏洞、越权访问漏洞、业务逻辑漏洞、Web框架漏洞、文件上传漏洞、弱密码、关联性漏洞等安全风险，一周内提供渗透测试报告，紧急情况需3天内提供渗透测试报告。  　　2. 渗透测试报告包含原因分析、解决方案以及校方要求的其他内容，协助校方进行漏洞、安全隐患等修复工作后进行复测。 | **服务范围:**学校提供的业务系统（不低于20个业务系统，不区分内外网，含复测，提供测试报告并协助做好整改工作)  **服务频率:**一年不少于2次（不含复测）  **交付物:**测试报告和整改工作 |
| 5 | 重要时期保障 | 1. 针对重大节假日、重大会议、大型活动、护网等重点保障时期，为校方提供专项保障服务，协助校方做好服务期内重要时期网络安全保障工作。  　　2. 服务将综合多年重大活动、会议期间的安全保障经验，对国内外非法势力的攻击方向和范围进行研究，以及校方实际网络安全情况，提供7\*24小时远程技术人员值守、网站监测、安全设备日志分析等服务，每日汇报安全情况，全程协助校方进行安全事件排查及调查取证工作。 | **服务频率：**根据学校要求响应  **交付物：**安全保障应急响应预案、安全保障工作日志、安全保障工作总结 |
| 6 | 应急响应 | 1.当校方网络与信息系统发生紧急安全事件时，迅速组织应急安全专家小组提供远程及现场支持，最快速处置事件，并采取有效措施，遏制事件蔓延并降低安全威胁事件带来的严重影响。  2.安全服务人员根据事件类别，通过远程和现场支持的方式协助校方对遇到的突发性安全事件进行紧急分析和处理。  3.应急响应服务应至少包括现场取证备查、事件分析、分析报告提交、问题解决建议等，保证重要系统能及时恢复上线。  4.驻场人员响应时间不超过0.5小时，应急安全专家小组远程响应时间不超过1小时，应急安全专家小组12小时内到达现场。 | **服务频率：**根据学校要求响应  **交付物：**网络安全事件应急响应报告、处置建议、协助进行安全事件处置 |
| 7 | 应急演练 | 通过应急演练服务，建立健全网络与信息安全运行应急工作机制，检验网络与信息安全综合应急预案的有效性，验证相关组织和人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力。同时，通过演练，不断提高各部门开展应急工作的水平和效率，发现不足，进一步完善应急预案。  根据实际业务环境，提供专项预案，准备演练场景，以模拟攻防演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。 | **服务频率：**不少于2次  **交付物：**应急演练预案（周期性完善）、应急演练方案、应急演练汇报 |
| 8 | 安全培训 | 根据校方的网络安全培训要求，提供网络安全培训课程，培训形式由校方指定，培训内容包含但不限于网络安全意识培训、网络安全管理培训、网络安全技能培训网络安全等级保护标准培训、商用密码应用安全性评估培训。 | **服务频率：**面向校内专业人员2次技术培训，面向师生2次知识讲座  **交付物：**技术培训、网络安全知识讲座、培训及相关文稿 |
| 9 | 网络安全宣传周宣传教育 | 根据国家网络安全宣传周的要求，协助校方开展网络安全宣传周各种形式的宣传，对师生开展网络安全教育活动。 | **服务频率：**不少于1年1次  **交付物：**网络安全宣传方案、组织过程、活动文稿等相关材料 |
| 10 | 安全预警 | 1. 密切关注零日漏洞、业界新发现的高危安全漏洞，针对高危安全漏洞及时预警，预警包括对安全漏洞的描述、影响范围、修复建议等内容。  　　2. 网信办、公安机关等相关的行业安全事件分析、安全规范解读、安全检查范围方法预警、通告。  　　3. 预警范围包含但不限于：应用安全漏洞通告、重大安全事件通告、采购方自身安全漏洞通告；通报时间7\*24小时，实时通报；通报后根据实际情况提供远程或现场技术支持。 | **服务频率：**根据学校要求响应  **交付物：**安全漏洞详情、修复建议、协助完成修复；安全预警通告及后续技术支持工作 |
| 11 | 安全咨询与策略优化 | 提供网络安全咨询服务，解答我校在网络安全建设、运维过程中的安全问题。同时，全面了解学校网络安全建设现状，参照国家及教育行业相关标准，协助我校制定网络安全建设方案和规划。根据等级保护要求和上级主管部门要求，协助学校制定、优化数据中心安全策略、互联网出口安全策略等;协助制定学校网络安全相关标准、制度，提供专业化安全建议。 | **服务频率：**根据学校要求响应  **交付物：**各类网络安全文件、制度、规范等，策略优化报告 |
| 12 | 安全威胁专项检查 | 根据上级主管部门要求、学校自行组织的各类网络安全专项检查，进行安全威胁检查，出具检查报告并协助做好相关威胁、漏洞等修复工作 | **服务频率：**根据学校要求响应  **交付物：**检查报告和修复工作 |
| **以上服务项及服务频率、交付物仅为本项目最低实施标准，必须全部满足。否则按无效投标处理。** | | | |

**三、服务要求**

1、满足服务内容中相关要求。

2、投标人在项目服务前，须详细分析在本次项目服务过程中存在的可能影响现有系统安全性与稳定性的风险，并采取必要的风险控制措施。任何由投标人在项目服务工作中对采购人造成的负面影响，其后果都须由投标人承担。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。

3、投标人中标后需要对信息安全做出承诺，对涉及的安全服务操作中的风险有专业的规避和防范措施，并能够对可能发生的信息安全问题承担责任。中标投标人提供项目实施期间信息安全保障机制，提供信息安全保障方案，确保采购人信息安全。因投标人工作失责导致的网络安全责任，由投标人承担相关责任。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。

4、项目实施前，签订保密协议；对项目实施中产生的数据和信息严格保密，未经授权不得泄露给任何单位和个人，否则招标人有权追究投标人的责任。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。

5、投标人承诺在中标后签订合同签订，详细分析在本次项目服务过程中存在的可能影响现有系统安全性与稳定性的风险，并采取必要的风险控制措施；并承诺由于投标人在项目服务工作中对采购人造成的负面影响，其后果都由投标人承担，提供相关承诺证明，格式自拟；

6、投标人承诺接受采购人在服务过程中对服务质量进行考核；接受采购人根据项目的工作计划安排，对阶段性工作成果进行审核；同时向采购人提交阶段性工作成果，以确保各阶段性成果及整个项目的质量，并提供相关承诺证明，格式自拟；

7、投标人须提供全天候7×24小时的技术服务，满足服务要求中对于故障抢修涉及的响应时间和故障处置时间的要求，并提供相关承诺证明。

8、驻场人员（工程师）具备不少于2年以上工作经验，熟悉网络技术、linux系列操作系统配置管理、网络安全技术，人员（工程师）入场前须经采购人审查通过方可驻场服务；在项目服务过程中，未经采购人批准，不随意更换工程师，如果采购人认为工程师不具备本项目所需的技术能力，采购人有权随时要求投标人进行更换，**投标时提供相关承诺证明。**

**四、采购需求其他相关要求及说明**

**1、为落实政府采购政策需满足的要求；**本项目落实政府采购促进中小企业发展政策、促进残疾人就业等政府采购政策。

**2、采购标的需满足的质量、安全、技术规格、物理特性等要求；**采购标的需满足的服务标准、期限、效率等要求；采购标的的其他技术、服务等要求：采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：略，详见采购需求（技术规格等）的主要要求。采购文件中的采购需求为主要要求或最低要求。投标人所供产品（服务）应当实质性响应招标文件的要求。采购标的有国家强制标准或财政部门强制要求的，投标人投标产品（服务）必须符合国家强制标准或财政部门强制要求(可以以产品质量标准合格代替)。采购标的没有国家强制标准的或招标文件未明确相关标准的，投标人投标产品应当符合行业标准、地方标准（江苏）等有关标准规范。在合同履行过程中，如有新的国家规定或标准规范出台的，投标人应确保所供产品符合新的规定或标准规范（因此而增加的费用与风险由投标人承担）。携手阳光公司所代理的政府采购项目中如涉及商品包装和快递包装的，应当符合《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。如投标人提供产品及相关快递服务的包装未达到其标准的，采购人有权拒收（视为履约验收不合格）。

**3、采购标的的验收标准；**

⑴驻场人员的工作日报、周报，项目阶段性工作的报告、报表，各类漏洞、安全事件处置的过程性文档，安全预警通告，培训资料，协助制定的各类制度、规范文件，及服务内容中所要求完成各类的预案、文稿等，要求内容记录完整、准确。

⑵全年网络及信息系统安全运行是否正常、安全服务质量是否符合采购人要求，服务质量考核表得分情况。

⑶采购人将根据招标文件的相关要求、投标人的投标文件（含承诺）以及采购项目的具体情况织项目验收。投标人应当确保一次性通过验收，如投标人未能一次性通过验收的，后期所产生任何费用（验收费等）及相关损失均由投标人承担（赔偿）。

⑷如投标人出现与投标文件（含承诺）不一致等情形的（服务未达到采购人验收要求的），采购人有权单方面解除合同（视为投标人不履约合同），投标人须承担由此对采购人造成的损失。

**特别说明：**

投标人应当充分了解采购人的采购需求以及需实现的功能或者目标等相关事宜。如采购人的采购需求存在描述不完整、表述不规范、含义不准确等情形的（未能达到法律规定明确的要求），投标人须在投标人须知规定的时间内，以电子邮件方式向携手阳光公司提出询问或要求进行澄清（以便采购人及时校正）。逾期视为投标人对采购人的采购需求无任何异议，并自愿一切以采购人理解、解释为准。