**附件1：**

网络安全运维项目技术要求

为了能保证网络平稳运行，减少网络故障，降低网络安全风险，高效快捷的推动各项网络及信息安全工作进行，现采用聘请专业运维团队提供驻场运维的形式保障工作正常开展，主要完成三方面工作：1.开展5个月网络及信息安全运维工作，期间安排一名工作人员驻场服务，完成日常维护、季度巡检、应急处置等工作；2.开展网络安全巡查服务，服务期间提供不少于3次渗透测试服务、不少于6次的安全风险评估服务；3.组织网络安全培训及网络安全应急演练各1次。详细技术要求如下。

**一、网络及信息安全运维**

**（一）网络运维**

1.信息化机房设备的运行与维护：网络安全设备、服务器、交换机等设备的维护与配置优化；机房环境的运行管理、相关技术咨询等。

2.办公网络系统的运行与维护：包括互联网和内网访问及网络故障处理；网络接口的开通与调整；新增办公终端的布线与网络开通；互联网和局域网的网络运行保障等。

3.系统安全的运行与维护：包括对网络出口的流量控制、上网行为管理控制、网络出口防火墙安全策略的调整与修改等。

4.运维软件升级：本次项目需要对河北省文物局定制开发的运维软件版本进行升级优化，提升运维软件自身性能，完善对信息系统的设备、链路状态监控，保障信息系统高可用性。

5.驻场运维工程师定期完成设备巡检：驻场运维工程师每周进行不少于1次的机房巡检服务，巡检过程中驻场运维工程师需填写巡检表单。对巡检过程中发现的问题或缺陷，应及时处理。驻场运维工程师应按季度提供运维服务报告，运维服务报告包括巡检表单及故障处理清单。

6.突发性需求响应服务：根据运维服务工作需要，有时需要临时抽调相关技术专家及原厂技术服务人员提供临时性服务，协助解决运维服务过程中出现的技术问题。

**（二）信息安全运维**

1.安全策略的制定和实施，如访问控制、安全审计、安全监控等。

2.安全事件的监测和响应，如入侵检测、入侵响应、安全事件管理等。

3.安全漏洞的扫描和修补，如漏洞扫描、漏洞修复、补丁管理等。

4.安全评估和审计，如网络安全评估、安全合规审计等，以确保网络安全和合规性。

5.协助完成等保测评、公安、网信及上级单位组织的安全自查工作。

**（三）服务期限**

自签订合同之日起5个月。

**（四）运维方式**

1.日常维护：要求提供7×8小时维修维护服务，服务期间保证通信畅通。保修应即时响应，1-2小时上门服务。

2.季度巡检：每季度提供一次全面的信息网络系统设备巡检服务，并出具巡检报告，根据实际情况提供信息网络系统维护方面的合理化建议。

3.驻场服务：每周周一至周五及重要节假日，安排1名专业运维人员提供驻场服务。驻场期间，需协助完成日常事务。运维人员应对信息网络系统进行设备巡查，及时发现故障隐患。

4.技术支持团队要求：本次项目要求4名专业技术人员组成技术团队，其中项目经理1名，网络安全工程师1名，网络工程师1名，驻场运维工程师1名。技术团队人员要求如下：

**项目经理：**对整体项目服务进行管理，负责运维服务统筹、协调和管理等全面工作，运维项目相关经验丰富。要求具有本科及以上学历，计算机相关专业，8年工作经验。

**网络安全工程师：**要求计算机相关专业，5年工作经验，熟悉病毒防范，熟悉防火墙系统、入侵检测系统、漏洞扫描系统等网络安全系统设备的配置和维护，熟悉主流网络操作系统、网络设备、服务器、PC 机等信息化设备的运维。

**网络工程师：**要求计算机相关专业，5年工作经验，精通路由、交换网络技术，精通 TCP/IP 协议，精通华为等网络设备的配置和维护，具有独立处理网络故障的能力。

**驻场运维工程师：**要求计算机相关专业，3年工作经验，熟悉主流网络设备、安全设备、服务器、PC 机等设备的运维；精通计算机机房基础设施运维相关知识，能尽快熟悉信息化机房的现状情况；有处理应急事件的能力和经验。

5.应急响应：遇有重大活动或信息网络系统发生重大故障时，需要提供即时响应服务（7×24小时，含周末、节假日），1小时内赶到河北省文物局指定地点，立即处理设备故障，提供现场技术支持服务。事件处理完毕后，交付《信息系统应急事件处理报告》和《信息系统安全事件分析报告》。

**二、网络安全巡查服务**

河北省文物局现有多个重要业务系统为单位内部办公和社会提供服务。因此，对于业务系统的安全防护非常重要。为了预先发现业务系统和资产中存在的潜在隐患，现需要向社会采购安全服务，主要针对业务系统的安全进行渗透测试、安全风险评估等一些服务，以此提高单位业务安全性和安全设备的防护效果。

**（一）渗透测试服务**

|  |  |
| --- | --- |
| **服务指标** | **服务参数** |
| 服务次数 | ★对指定的业务系统提供不少于3次渗透测试服务，渗透方式可以为本地渗透或远程渗透。 |
| 服务简介 | 在保证客户信息系统正常运行前提下，模拟黑客攻击行为信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞。帮助客户理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全。 |
| 交付成果 | 包括但不限于：过程文档及正式的《渗透测试报告》。 |
| 服务方案 | 根据安全需求及重要业务系统结构，设计有针对性的渗透测试方案；支持在测试前，详细说明渗透测试的实施流程、渗透测试方法、实施过程中用到的工具、实施过程中可供考量的具体工作指标及各阶段输出成果。 |
| 渗透测试工作内容 | 网络及安全设备渗透； |
| 主机操作系统渗透； |
| WEB应用系统渗透； |
| 数据库系统渗透； |
| 提供的渗透测试服务方案 | 渗透方法和流程； |
| 渗透测试风险评估和控制方案； |
| 渗透测试须采用国内外商业检测工具或自有检测工具。 |
| 对于一类系统采用新的渗透测试方法，渗透测试方式多样化，创新测试方法，针对的业务特点，定制合理的测试方案。 |

**（二）安全风险评估服务**

| **服务指标** | **服务参数** |
| --- | --- |
| 服务次数 | ★对指定资产累计提供不少于6次的安全风险评估服务。 |
| 资产识别 | 依据相关国家标准或国际标准，对客户的资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等； |
| 资产类别应按照相关规范分类，包含但不限于业务应用、网络结构、数据文档、软硬件资产、物理环境、组织管理。 |
| 脆弱性识别 | 依据相关国家标准或国际标准，根据资产识别结果，采用不同手段对资产进行全面的脆弱性识别，及时发现、处置脆弱性，避免或降低脆弱性被利用的几率； |
| 脆弱性分类应至少包括但不限于以下三类：技术性弱点—系统、程序、设备存在的漏洞或缺陷，如网络结构设计问题和代码漏洞；操作性弱点—软件和系统配置、操作中存在的缺陷，包括人员在日常工作中的不良习惯，审计和备份的缺乏；管理性弱点—策略、程序、规章制度、人员意识、组织结构等方面的不足。 |
| 漏洞扫描 | 应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 |
| 漏洞扫描工具支持对象应包含但不限于：网络设备、操作系统、数据库、中间件。 |
| 提供的漏洞扫描工具应具备对高可利用漏洞的管理，提供的漏洞扫描工具应具备对扫描出或已修复的漏洞，具备一键复测功能。 |
| 基线核查 | 对基线核查的资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 |
| 基线核查应包含但不限于以下内容：网络设备、操作系统、数据库、中间件。 |
| 威胁识别 | 依据相关国家标准或国际标准，对存在脆弱性的资产进行威胁的全面识别，及时发现潜在威胁的原因，避免或降低威胁发生的几率。 |
| 威胁来源应至少包括但不限于以下四类：人员威胁、系统威胁、环境威胁、自然威胁。 |
| 应对威胁利用率极高的风险提出整改建议，配合客户及时处置。 |
| 风险分析 | 对存在和潜在的风险进行全面分析，保证风险分析的科学性、合理性及风险处置的可操作性。 |
| 在风险分析完成后，将风险评估实施过程全生命周期发现的情况或问题统一反馈，并提出可落地的建议或方案。 |

**三、安全培训及应急演练**

**（一）安全培训**

1.网络安全意识培训：培训内容包括网络安全的基本概念、常见的网络威胁和攻击方式，以及如何识别和应对这些威胁。培训可以通过面对面的讲座、在线课程、视频教程等形式进行。

2.信息安全政策培训：培训内容包括组织的信息安全政策和规定，包括密码安全、数据保护、网络访问控制等方面的要求。培训可以通过讲座、培训课程、在线学习平台等方式进行。

3.电子邮件和通信安全培训：培训内容包括电子邮件和其他通信工具的安全使用方法，包括识别和防范钓鱼邮件、恶意软件等网络威胁。培训可以通过案例分析、模拟演练等方式进行。

4.移动设备安全培训：培训内容包括移动设备的安全使用方法，包括密码设置、设备锁定、应用程序下载等方面的知识。培训可以通过讲座、培训课程、实践操作等方式进行。

5.社交媒体和网络安全培训：培训内容包括社交媒体的安全使用方法，包括隐私设置、信息分享注意事项等方面的知识。培训可以通过案例分析、讨论会等方式进行。

6.数据安全培训：培训内容包括数据安全意识培训、影响数据安全的因素分析及日常保障数据安全的方式等数据安全知识。培训可以通过案例分析、实践操作等方式进行。

7.共组织安全培训1次。

**（二）应急演练**

1.演练目标和场景：明确演练的目标和场景，例如网络攻击、自然灾害、数据泄露等，以确保演练的针对性和实用性。

2.应急响应流程：演练应急响应流程，包括事件识别、报告、调查、应对和恢复等步骤，以确保演练的连贯性和高效性。

3.通信和协调：演练组织内部和外部的通信和协调机制，包括内部通知、外部合作等，以确保演练的协同性和透明度。

4.演练参与者培训：对参与演练的人员进行培训，提高其应急响应能力和技能，以确保演练的效果和质量。

5.演练评估和总结：对演练进行评估和总结，分析演练中存在的问题和改进的空间，以提高组织的应急响应能力。

6.共组织应急演练1次。

附件2：

网络安全运维项目评分标准

|  |  |  |
| --- | --- | --- |
| **评审项目** | **标准分** | **评分标准说明** |
| 报价得分 | 10 | 满足比选文件要求且响应价格最低的报价为评审基准价，其价格分为满分10分。其他供应商的报价得分统一按照下列公式计算：报价得分=（评审基准价／响应报价）×10**备注：未实质性响应采购文件要求的供应商的响应报价不参与报价得分的计算。** |
| 项目理解和思路 | 15 | 根据供应商对本次服务需求的理解情况及策划实施思路，重难点分析情况进行综合评价：（1）对本项目详细分析、理解透彻，重点、难点判断准确、 描述清楚，思路清晰、可行性高，得15分； （2）对本项目进行分析，重点、难点有一定理解和阐述，思路较为完整，得12分； （3）对本项目具备初步分析、理解，思路和可行性一般，得9分；缺项，得0分。 |
| 整体服务方案 | 25 | 根据供应商提供服务方案的服务内容合理性、合规性等进行综合评价：（1）服务方案合理，内容详细，措施完善，可行性强，完全满足或优于采购要求，得25分；（2）服务方案较合理，内容较详细，措施合理，可行性较好，达到采购要求，得20分；（3）服务方案内容一般，具备一定的可行性，基本符合采购要求，得15分；缺项，得0分。 |
| 组织结构及项目团队 | 10 | 根据供应商项目实施团队的组织结构和人员配备情况进行综合评价：（1）组织管理机构完善、合理，团队人员构成专业性强、经验丰富符合项目特点的，得10分；（2）组织管理机构健全、合理，团队人员构成和专业性较好，相关经验较丰富，符合项目需求的，得8分；（3）组织管理机构和人员构成基本合理，专业性和相关经验稍有欠缺，得6分；缺项，得0分。 |
| 服务承诺及保障措施 | 15 | 根据供应商的服务承诺与保障措施进行综合评价：（1）服务保障体系及措施完善，技术支持能力强，保证措施完善，得15分；（2）服务保障体系及措施较好，技术支持能力较强，保证措施较完善，得12分；（3）服务保障体系及措施基本符合采购要求，技术支持能力和质量保证措施一般，得9分；缺项，得0分。 |
| 进度安排及保障措施 | 10 | 根据供应商进度安排及保障措施进行评审：（1）进度安排科学合理、保障措施完善、可行性强，得10分；（2）进度安排较科学合理、措施较完善、较可行，得8分；（3）进度安排基本符合采购需求，保障措施及可行性一般，得6分；缺项，得0分。 |
| 应急预案 | 10 | 根据供应商应急预案优劣进行综合评价：（1）应急预案科学、合理、完善可行，有针对性，得10分；（2）应急预案较科学、较合理、较完善可行，得8分；（3）应急预案一般，可行性一般，得6分；缺项，得0分。 |
| 同类项目业绩 | 5 | 供应商自2021年9月至今（以合同签订时间为准）与最终用户签订的同类项目业绩，每具有一份同类项目业绩加1分，满分5分，提供合同复印件或扫描件。 |

评分说明： 供应商综合得分为所有评委打分的算术平均值。