**附件：**

**服务内容及要求**

**1、项目服务列表：**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **周期/次数** |
| 1 | 信息安全等级保护测评服务 | 3套二级系统 | 一次 |
| 2 | 渗透测试与远程扫描服务 | 不少于四次 |
| 3 | 网站系统安全实时监控服务 | 7X24小时 |
| 4 | 信息安全应急响应服务与应急事件处置服务 | 不限次数 |
| 5 | 网页防篡改产品服务iGuardV3.0标准服务（2套） | 升级及不少于四次巡检 |

**2、项目服务内容：**

为了从各个方面加强信息安全保障，全面提高深圳市罗湖区人民法院整体信息安全水平，本次项目的内容主要包括信息安全检查和运维保障、网站系统实时安全监控和信息安全等级保护测评等服务工作。

**1）、信息系统等级保护测评**

根据《信息系统安全等级保护基本要求》（GB/T22239-2008）相关要求，对深圳市罗湖区人民法院以下重要信息系统进行等级保护测评，认真查找各个层面存在的安全问题，提出专业的整改建议和方案，并出具符合国家等级保护要求的测评结果报告。

**1.1）、测评内容**

信息系统的安全等级测评内容应包括技术和管理两大类，其中技术类应包括对物理安全、网络安全、主机安全、应用安全和数据安全及备份恢复等方面的测评，管理类测评应包括对机构安全管理机构、人员安全管理、安全管理制度、系统建设管理和系统运维管理等方面的测评。

**1.2）、测评范围与对象**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 系统等级 | 全年服务次数 |
| 1 | 法律文化书院系统 | 二级 | 1次 |
| 2 | 官方门户网站系统 | 二级 | 1次 |
| 3 | 微信公众平台系统 | 二级 | 1次 |

**2）、渗透测试与远程扫描服务**

针对外网业务应用系统进行模拟黑客使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，挖掘应用系统层面的安全漏洞，测试漏洞的可利用性和造成的安全风险。应用层的渗透测试主要针对B/S、C/S等架构的系统，是当前最流行的攻击手段。大部分黑客入侵都是由此开始，并渗透到系统和网络。

从信息安全风险管理的角度出发，通过漏洞扫描工具检测、漏洞知识库搜集和人工分析的技术手段，全面评估重要服务器、应用系统、中间件、数据库网络设备和安全系统等资产存在的安全漏洞、弱口令及其关联性和影响程度，并形成基础网络与信息系统的整体脆弱性的专业性安全服务。

对安全检测结果中发现的系统弱点（漏洞、配置隐患）、管理缺陷等一系列安全问题，提出可行的整改建议，为我院开展整改提供咨询，提高系统安全性和风险管理水平。

**3）、网站系统安全实时监控服务**

根据上级单位《深圳市政府网站建设与管理规范》的相关要求，对网站系统运行状况、网页规范化、内容非法篡改、挂马、黑链等提供一年7X24小时安全监控，及时发现并协助深圳市罗湖区人民法院进行处置。

**4）、信息安全应急响应服务与应急事件处置服务**

具有应急服务中心为我院提供7\*24小时多种方式的安全事件应急服务。一旦我院外网信息系统因非法攻击或病毒入侵等原因而遭到破坏、更改或泄露，造成系统不能正常运行，或已经发现的有可能造成安全事件的隐患，如非授权访问、信息泄露、系统性能严重下降、蠕虫或大面积爆发病毒等。应急服务中心工程师将第一时间到达指定现场协助解决问题，防止安全事件影响进一步扩大。

**5）、网页防篡改产品服务iGuardV3.0标准服务（2套）**

需提供以下维护服务内容：

* 解答问题：解答在安装、配置和使用产品的过程中出现的疑问和问题；
* 接受反馈：接收有关产品缺陷和错误报告，以及对产品提出的改进建议；
* 提供补丁：对于本产品存在的缺陷或错误，将不定期提供最新的补丁；
* 系统咨询：提供与产品相关的系统安全方面的简要咨询与现场服务。

**3、项目实施要求：**

**1）、项目周期及计划要求**

此项目为长期服务项目，本次合同服务时间：2018年1月至2018年12月31日。如满足《罗湖法院外网信息系统安全服务项目服务质量考核标准》（附后）续签合同标准，可按原合同内容续签2年。

项目应严格按照当年国家信息安全等级保护相关要求以及满足深圳市罗湖区人民法院信息安全保护需求按期、按质执行，确保在规定的时间内完成各项检查和完善工作。

**2）、项目交付要求**

项目中各项安全服务结果必须真实、可靠、全面，满足本年国家信息安全等级保护标准要求；

项目实施过程产生的所有过程文档、检查记录、人员访谈纪要、检测原始数据、服务结果报告等必须进行电子和纸制双重归档，根据要求，整理成册，并及时交付深圳市罗湖区人民法院。

**3）、项目资源要求**

为确保信息安全服务项目的有效落实，合作方需具备全面的项目管理能力，对于项目各项服务内容要求、实施计划与质量控制、风险评估与分析、专项问题分析与咨询等方面，提出完整的管控方案。

3.1）、应当按计划合理配置人员进行安全服务实施；

3.2）、应当由专人进行项目管理与跟踪。

**罗湖法院外网信息系统安全服务项目服务**

**质量考核标准**

为了规范厂家维护服务流程，加强对厂家服务质量的考核，客观、公正地评价厂家服务质量，督促厂家不断改进服务质量，提高深圳市罗湖区人民法院（以下简称罗湖法院）《罗湖法院外网信息系统安全服务项目》维护质量，特制定本考核标准。

**一、服务质量考核内容及得分计算方法**

《2018年罗湖法院外网信息系统安全服务项目》中包括了如下五个子项目服务：

|  |  |
| --- | --- |
| 信息安全等级保护测评服务 | 3套二级系统 |
| 渗透测试与远程扫描服务 |
| 网站系统安全实时监控服务 |
| 信息安全应急响应服务与应急事件处置服务 |
| 网页防篡改产品服务iGuardV3.0标准服务（2套） |

服务考核要求：按照《罗湖法院外网信息系统安全服务项目》中指定的服务范围，在按时完成定期服务项目，按需完成不定期服务项目的基础上，来考核安全服务质量。

服务质量考核内容包括四部分：服务项目完成质量、服务响应及时率、服务 规范性、服务满意度。

服务质量界定：由于乙方技术不到位或者是操作不当，或者是乙方未及时提 醒/通知甲方，或者是乙方未积极协助配合支撑而造成的安全服务质量问题。

计分公式：服务质量考核得分 = 服务项目完成质量(60分) + 服务响应及时率(20分)+ 服务规范性(20分)

服务质量考核三个分项内容的考核方法如下：

1、服务项目完成质量（60分）

服务项目完成质量考核计算方式：总分60分，出现服务质量问题时逐项扣分，扣完为止的方式来计算分数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 扣分项 | 详细描述 | 扣分规则 | 扣分 |
| 1 | 服务缺失 | 未完成安全服务子项目，或者没有完成该子项目下的服务。归为 5 个子项目服务：信息安全等级保护测评服务、渗透测试与远程扫描服务、网站系统安全实时监控服务、信息安全应急响应服务与应急事件处置服务、网页防篡改产品服务iGuardV3.0标准服务（2套） | 每个子项目中一次服务都没有实施，定义为子项目服务缺失，每缺失一个子项目服务，扣20分（子项目无服务需求，则不扣分。如应急响应服务，甲方无服务需求，不扣分,而甲方提出了需求，乙方未及时提供或者不能提供服务，扣20分），子项目中服务次数缺失，是指子项目中规定的服务次数没有达到，缺失1次扣5分。如缺失服务引起业务运营中断或者严重影响罗湖法院形象，1次扣30至60分，甲方有权终止合同 |  |
| 2 | 服务范围 | 服务范围未能满足安全服务项目中甲方指定范围 | 未满足1次扣5分 |  |
| 3 | 高危漏洞 | 在渗透测试和安全评估服务中未能发现已存在系统中的严重安全威胁(高危漏洞已经是业界共识，并且已经发布一个星期以上时间) | 未引起安全故障扣 1 分；导致安全故障扣5分；影响到运营业务扣 10 分；严重影响到运营业务扣30分 |  |
| 4 | 病毒/木马和入侵 | 在渗透测试和安全评估服务中未能发现网站被入侵，或者是系统已中病毒和木马（这些病毒和木马以及漏洞已经是业界共识，并且已经发布一个星期以上时间） | 未引起安全故障扣 1 分；导致安全故障扣5分；影响到运营业务扣 10 分；严重影响到运营业务扣30分 |  |
| 5 | 解决安全问题 | 在发现安全威胁（漏洞、病毒、木马、入侵、补丁）而未能提供有效解决方案，或未积极配合、未通知到甲方去加固,或未能解决安全问题 | 未引起安全故障扣1分，导致安全故障扣5分；严重影响到运营业务扣10到30分 |  |
| 6 | 重复的安全问题 | 同一主机（系统、应用）重复出现同样的安全问题 | X 的 N 次方扣分：1)未引起安全故障 X=1；2)引起安全故障 X=2；3)影响到运营 X=4；4)严重影响运营 X=6分；其中 N 为重复次数 |  |

2、 服务响应及时率（20 分）

服务响应及时率考核计算方式：总分20分，出现服务质量问题时逐项扣分，扣完为止。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 扣分项 | 详细描述 | 扣分规则 | 扣分 |
| 1 | 安全服务子项目完成及时性 | 以上所列安全服务子项目在实施过程中，因未能及时处理，而导致安全问题 | 1）未引起安全故障扣 1 分；2）导致安全故障扣 5 分；3）影响到运营业务扣 10 分；4）严重影响到运营业务扣 30 分 |  |
| 2 | 应急响应 | 响应时限：发生安全事件需现场技术支持时，工程师2个小时内到达现场；处理时限：尽量在不影响业务运行情况下，处理安全应急事件；出现系统瘫痪或者需要重启，保障重要业务平台2 小时内恢复正常运行；主要业务平台，2 小时内恢复正常运行，其余业务平台不超过 4 小时恢复正常运行 | 1）工程师未能在 2小时到达现场，扣5分；2）重要业务平台恢复时限内多超 1 个小时多扣 20分；3）主要业务平台恢复时限内多超1个小时多扣10分；4）其余业务平台恢复时限内多超 1小时多扣5分 |  |
| 3 | 安全通报和信息安全预警 | 安全通报、信息安全预警、互联网恶意信息调查未及时提供 | 超过1个周期扣1分（周报、月报和季报） |  |
| 4 | 技术支持和安全咨询 | 技术支持和安全咨询及时反馈 | 超过 1 天，扣 1 分 |  |

3、 服务规范性（20分）

1）项目管理规范性(10分) 要求：组织架构合理，管理制度规范，工作流程和工作范围明确，服务人员的资质符合事先规定。如出现未按照既定的要求或服务过程中无端进行人员变动等情况，则每次扣 2 分。

2）项目执行规范性（10 分）

a.阶段性服务报告和年终服务报告，未提供每次扣3分，未及时提供每次扣1分；

b.应急响应报告必需在安全问题消除后两天内提交，否则扣 2分。

**二、服务质量考核结果处理**

乙方应承诺服务质量考核得分高于或等于 90分，甲方根据乙方服务质量考核得分进行如下处理：

1、当乙方的服务质量年度考核得分高于或等于90分，甲方按合同额的100％向乙方付费，并给予本项目合同100%的续约合同与金额保证，当服务内容发现较大变化时双方在另行商榷。

2、当乙方的年度服务质量考核得分低于90分时，每低1分，甲方有权从合同付款约定中扣除合同额的1％比例的费用，但总的扣除费用不超过合同总额的 10％。

3、当乙方得分低于 80分时，甲方有权终止合同。

**三、有关服务质量的其他要求**

当服务质量没有达到甲方所选择的服务所规定的服务质量指标时，甲方有权要求乙方继续提供服务，直到问题解决为止。

如因乙方服务质量问题造成甲方损失，甲方保留其他索赔权力。