**1.项目需求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务 项 目 | 数量 单位 | 服务内容及要求 |
| 1 | 信息  化运  维服  务外  包项  目 | 1项 | 一、维保服务工作范围  (一)网络安全运维：负责对中心信息化系统硬件及应用系统(主要包括计  算机终端、服务器、安全设备、网络设备以及应用系统)进行资源整理、网络规划以及  网络安全运维等，主要包含网络资产核查与网络拓扑优化升级、优化网络、 定期驻守安全运维、安全检测、安全加固、应急响应、安全日志分析和处置、 风险评估以及信息化建设咨询等服务。  (二)机房基础设施运维：负责中心计算机机房(数据中心机房、备份机房、 视频机房)定期维护、巡检及故障处理工作，网络设备及网络线路的日常运 维及配置，确保中心整个网络信息系统基础设施的正常运行。按照业主实际 工作需求，提供现场巡检、维修调试、故障恢复、操作系统的安装、现场培 训等服务，及时发现并及时协调技术团队处置问题。。  (三)办公电子设备运维：负责采购人办公电子设备(台式电脑、笔记本电  脑、打印机、扫描仪等)维修保养具体工作实施，安排专业技术人员驻场开 展设备日常维保工作，及时处理中心各科所提交的设备维修申请，修复设备 或网络故障，提高维保工作效率，确保中心办公电子信息设备正常使用。  (四)应急演练与培训服务：提供网络安全知识、电子设备维护保养知识、 安全攻防技能等培训服务；提供网络安全攻防实战应急演练，以提升单位人 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。  二、维保服务工作周期及预算  维保服务工作周期为：2年，合同采用一年一签的形式。  三、维保服务主要工作内容  (一)网络安全运维服务：1项  1、资产核查与网络拓扑优化升级服务：对现IT机房资源进行检查(资产，  拓扑，网络架构，系统架构)等整理。提供虚拟化网络工程师服务，CISP注 册信息安全专业人员配合。  2、优化网络：优化与规划网络架构，提出合理化整改方案，包含拓扑优化， IPV6规划，统一管理优化，安全优化等方案，包含应用系统、服务器、平台 软件，存储备份、网络安全，基础设施做详细整理和优化方案，出具整体网 络优化与系统安全方案建议书。  3、定期驻守安全运维服务：  (1)提供驻场技术人员负责网络及应用系统的安全运维服务，每周提供不少 于2人 ·2天的现场驻守服务。(此2名技术人员为网络安全运维专业人员，  不与长期驻场办公电子设备运维人员重叠。)  (2)按采购人需求提供重要时期值守服务(不限于春节、两会、五一、国庆  节、东盟博览会等节假日期间，以及上级部门开展网络安全巡检前，不少于2 人 ·天的现场服务，提前进行现场安全驻场或提供远程值守(视单位工作情况) 支持)。  (3)提供护网行动期间的全程驻守服务，具体内容包括服务器安全维护、安 全设备运维、安全设备策略调整优化、安全日志分析、重大时期安全保障服 务。  4、安全检测服务：  (1)提供漏洞扫描及渗透测试服务，对机房现有的服务器、数据库、网络/  安全设备、web应用等进行安全分析，提出整改建议并协同进行整改修复。漏 描频次：≥12次，每月不少于1次；渗透测试频率：每半年1次；系统数量  >10个。  (2)定期对外部或内部的关键业务系统进行模拟黑客攻击的安全测试，全面 |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | 评估业务系统的脆弱性，评估现有安全防护体系下的业务系统的整体的安全 状态，并提供安全处置建议和指导进行修复。  (3)提供服务器(包括但不限于：数据库服务器、应用服务器、虚拟化服务 器、WEB/网管/备份服务器、防病毒服务器等)安全维护，维护内容包括但不 限于：1)对安全管理应用进行定期的维护，如防病毒软件的防护状态与病毒 库更新情况进行定期检查；2)服务器操作系统漏洞定期检测和修补；3)木 马病毒定期扫描与处置。  (4)提供安全设备(包括但不限于防火墙、IPS、IDS、WAF、态势感知等安 全防护和监测类设备)的运行健康检查和特征库升级检查，维护内容包括但不限 于：1)设备硬件状态检查、如CPU、内存、硬盘占用等情况；2)安全设备病 毒库更新和升级检查。  **5、安全加固服务：**  (1)提供按需安全加固，主要是根据风险评估、等保测评结果进行系统安全 调优服务，根据根据等保合规要求调整各类主机、网络、安全设备策略配置， 从技术和管理方面两方面进行整改加固。  (2)提供主动安全加固，在未出现安全事故之前就对已经通报或者暴露出来 的软件漏洞或最新病毒库更新，就主动进计划的升级和改进，从而避免出现 安全事故。  (3)提供安全加固内容包括但不限于：口令策略、协议安全、登录失败处理、 剩余信息保护、用户权限分配、系统服务策略、补丁管理、日志配置等。  **6、应急响应服务：**根据采购人收到的网络安全风险预警或受到的网络安全突 发事件对安全事件进行分析排查，阻断正在进行的攻击，封堵入侵途径，对 攻击进行溯源，分析攻击入侵后的系统安全状况和系统存在漏洞，并给出解 决方案并协同进行整改修复。服务频次：按需。  **7、安全日志分析和处置：**定期对防火墙、IPS、WAF、态势感知等安全设备产 生的安全日志进行收集，综合对这些日志进行关联分析，针对发现的安全威 胁进行上报和处置。  **8、风险评估服务：**提供运维阶段的风险评估，评估内容包括对真实运行的信 息系统、资产、威胁、脆弱性等各方面。  **资产评估：**对真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、 系统运行过程中生成的信息资产、相关的人员与服务等。  **威胁评估：**真实环境中的威胁分析，应全面地评估威胁的可能性和影响程度。 对非故意威胁产生安全事件的评估可以参照事故发生率；对故意威胁主要由 评估人员就威胁的各个影响因素做出专业判断；同时考虑已有控制措施。 **脆弱性评估：**全面的脆弱性评估。包括运行环境下物理、网络、系统、应用、 安全保障设备、管理的脆弱性。采取核查、扫描、案例验证、渗透性测试的 方式验证脆弱性；采取文档、记录核查进行验证。  **风险计算：**根据相关标准，对主要资产的风险进行定性或定量的风险分析， 描述不同资产的风险高低状况。  **(二)机房基础设施运维管理：1项**  **1、机房环境监测与运维**：设备包含但不限于消防系统、动环监控系统、UPS 不间断电源、门禁系统、精密空调等。  **UPS(不间断电源)维护(艾默生4组电池柜60KVA)**:定期进行UPS主机及  电池组检测，如UPS与市电线路之间的切换试验。对未接入UPS的关键设备 进行线路的调整；检查记录UPS运行参数，为用户提供整改完善意见和建议。 **机房精密空调与配电设备维护**(2台艾默生、2台海瑞弗精密空调以及新风系 统):定期检查空调设备、新风设备、主配电箱。调整精密空调设备的运行 参数，保证机房始终处于适宜温湿度环境下运转；检查空调运行是否正常， 换风设备运转是否正常，检查否缺少制冷剂。检查空调压缩机高、低压保护 开关、干燥过滤器及其他附件。  **消防设备维护**(3组柜式七氟丙烷灭火装置):定期检查检查火警探测器、手 动报警按钮、火灾警报装置外观及试验报警功能；检查火灾警报控制器的自 |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | 检、消音、复位功能及主备用电源切换功能。  **门禁系统维护：**定期对门禁系统进行检查，确保门禁电源、电压等是否正常 运转。确保密码、人脸、磁卡验证功能正常可用。  动环监控系统维护：定期检查动环监控系统的运行情况，发生报警及时处理。 机房环境养护(约20组机柜):定期对机房内部的关键信息基础设施进行除 尘处理；每季度至少开展一次机房环境保洁，静电地板清洁，地面除尘、缝 隙调整；检查吊顶，检查电路及照明，接地电阻测试；主接地除锈、接口紧 固；防雷器检查；接地线路防氧化加固。  **2、机房设备运维：**设备包含但不限于防火墙、交换机、WAF、服务器、存储 日志服务器、沙箱、全流量分析、备份一体机、态势感知、虚拟化安全、终 端安全管理、集中管理等50多台。  (1)确保机房内关键基础设备处于正常运行状态，定期进行硬件状态检查、 系统状态检查、线缆连接情况检查，维修故障部件。  (2)协助采购人开展应急故障处理、系统运维管理、系统升级、病毒查杀、 网络配置等工作。  (3)定期做好各种重要数据和系统的备份，当数据受损坏时，应提供数据恢 复方案，并尽力提供无偿恢复服务。  (4)对机房内所有设备每季度至少开展一次全面的保洁工作。  **3、网络设备运维：**网络设备包含但不限于核心交换机、约100台楼层交换机、 约260台无线AP以及网络线路等：  (1)定期对中心内部网络进行测试，按需对交换机等网络中继设备进行配置 调整、性能调优等，保障网络顺畅、稳定。  (2)对网络核心设备做日常维护，检查设备运行状态、物理状态。  (3)定期检查设备的系统日志文件，系统错误记录，分析系统存在的问题并 解决问题。  (4)重大故障调度配合、及时到场协助抢修。  (5)机房网络设备及线路巡检服务：提供现场巡检服务，并按时提供巡检报 告。  (6)网络线路日常维护，局域网的资源规划、IP设置、日常运维及设备管理。  **(三)办公电子设备运维服务：1项**  **技术人员须驻场对PC、笔记本等办公电脑(约700台),以及打印机、复印** **机、扫描仪等其他办公电子设备(约200台)的提供日常运维和故障处理等** **服务。**  (1)派驻不少于2名技术人员长期驻场提供办公设备的运维服务。  (2)故障检查与维修：包含计算机硬件拆卸组装；各类外设安装和维护；系 统软件、操作系统安装、应用软件安装及维护；打印机、复印机的维修保养、 故障处理及耗材零件更换，安装驱动，设置共享等。  (3)日常运维：办公电子设备进行除尘、保洁；电脑系统各类软件升级；驱 动程序安装；病毒查杀和防范；重要数据的备份；设备使用的培训。  (4)电脑网络故障诊断排除及维护管理，网络设备安装、设置、调试及检测。  (5)建立电子信息设备技术档案。  **(四)应急演练与培训服务：1项**  **1、提供安全培训服务：**培训分为网络安全意识培训、电子设备维护保养知识 培训、安全事件应急演练培训、安全攻防技能培训。服务次数：1次；培训时 间：1天。  **2、提供应急演练服务：**提供网络安全攻防实战应急演练，以提升单位人员应 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。  **四、维保工作要求：**  **(一)驻场服务**  1、提供至少4名技术工程师驻场服务(a.负责办公电子设备运维的技术人员 至少2人提供每周5天×8小时驻场服务；b.负责网络安全运维的技术人员2 人提供不少于每周2天×8小时驻场服务),按采购人时间上下班，工作地点 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 为南宁市金洲路18号、桃源路80号。人员要求大专以上信息技术相关学历， 35岁以下，至少3年或以上IT相关从业经验，具备包括终端主机、网络、机 房设备维护的工作经历、技能以及相关专业资质，熟悉Windows、Linux等操 作系统及电脑外设、打印机等软硬件日常安装、维护故障处理，熟悉网络设 备安装调试。服务期间必须遵守中心制定的各项关于机房设备及业务系统运 维的管理制度，并需要签订保密协议。  2、驻场工程师保持相对固定，不得随意更换，全年(包括所有的节假日期间) 提供不少于2名工程师在常驻本地，确保满足响应时间要求，协助用户制订 日常运行管理规范和设备运行应急预案；当现场工程师及其他支持方式无法 解决问题或技术力量不足时，服务方应及时提供后援技术支持和补充。合同 期间如更换驻场人员，均需符合上述资质要求，如有不称职的要及时更换。 3、供应商技术团队技术人员中需有人员具备以下资格：网络认证证书、网络 安全工程师认证证书、信息安全认证工程师等。  **(二)定期巡检：**按照工作计划要求，定期对系统进行预防性维护，包括检 查系统状态、设备清洁、系统备份，以及与客户工程师的技术交流，并提供 巡检报告。  **(三)服务响应及技术支持：**一般性故障由驻场工程师负责处理，在15分钟 内响应采购人的维护请求，30分钟内到现场处置(含节假日期间),重大活  动时驻场工程师全天现场待命，一般故障应在到达现场后的2小时内解决。  如遇驻场工程师无法处理重大故障，维保公司技术支持团队应在2小时内到 达现场，重大故障应在到达现场后4小时内解决，协助采购人完成故障定位 和处置工作，必要时协调相关厂商技术人员进行技术支持并负责相关人员的 费用，所需费用包含在本次采购报价里，不另行支付。  **(四)提供部分备品备件及相关耗材**：在本地储备相应设备维保的备品备件 及相关耗材(如网线、水晶头、电源线、数据线、电池等),确保在出现故  障时，及时更换。所需费用包含在本次采购报价里，不另行支付。  ( **五)提交服务报告：**根据信息管理部门要求提供服务报告，产生不限于以 下的记录和服务报告： | | | | |
|  | **服务** | **报告内容** | **提交时间** |  |
| 日常运维服务报告 | 运维月/季/年报告 | 月度/季度/年度 |
| 重大事件服务报告 | 重大事件服务报告 | 按事件发生情况 |
| 巡检报告 | 每日安全巡检工作记录 | 周/月度 |
| 设备维修 | 设备维修单 | 每周5天×8小时驻场 其余时间电话/远程 |
| 系统/网络优化分析 | 网络拓扑图、系统/网络优化建议 | 按用户计划 |
| 网络安全运维报告 | 病毒检测处置记录、补丁修复记录、 漏洞扫描报告、渗透测试报告 | 每周2天×8小时驻场 其余时间电话/远程 月度/季度/年度 |
| 风险评估报告 | 风险评估运维评估 | 月度/半年 |
|  | | | | | | | |
|  | | |  | | | | |
|  | | |  | | | | |
|  | | |  | | | | |