**2021年度网络安全技术运维服务项目**

## 项目概况

鉴于当前国际及国内对网络安全发展的大趋势、大环境，政府机关的网络安全由于历史发展的原因，备受关注。2014年以来，发生在浙江省内政府机关的网络安全事件屡见不鲜，对我省政府机关的风络安全现状提出了严峻的考验。杭州市规划和自然资源局萧山分局管理着不动产登记、审批系统、档案系统等多个业务信息系统，机房现有PC服务器、存储、数据备份以及网络安全设备等多套，这些设备支撑着这些信息化业务系统的稳定可靠运行。随着业务信息数据的急剧增长，本单位信息化系统各种安全风险和压力都比较大，为进一步加强分局的信息运维管理，保障分局内信息系统安全稳定运行，提高信息系统事件快速响应及处理能力，现提出信息技术支撑服务需求，通过信息技术支撑服务提供有效的信息系统安全保障，保证系统的性能满足业务发展的需求、满足7x24小时高可靠运行的业务连续性要求、保证数据的安全性和可恢复性，避免因硬件故障、网络安全风险等造成数据丢失或业务中断问题引起的各类业务纠纷，降低政府负面影响。

## 项目范围及服务期限

本项目服务范围：杭州市规划和自然资源局萧山分局机房内所有信息化设备（包括网络安全设备、服务器、UPS、气体灭火等）日常技术支撑运维（含服务期间新上设备）、机房环境监控、设备固件及杀毒软件升级，并提供现场驻点服务。

本项目服务期限： 2021年全年。

## 项目要求

本次项目安全服务要求包含以下部分：

1. 对过保安全设备提供保修服务、特征库升级及第三方安全运维服务。
2. 对过保网络、IT设备提供第三方安全运维及有偿硬件维修服务。
3. 对未过保设备提供第三方安全运维服务。
4. 驻点工程师需拥有出色的学习能力，具备CCNP以上网络能力，能吃苦耐劳，夜间出现系统问题也能第一时间响应，熟悉各类数据库及各类操作系统，逻辑排障能力强，熟练掌握ArcGIS软件，能够分担分局信息化日常工作。
5. 重要历史时期现场值守服务：在重要的时期（如春节、五一、国庆安保值守、重大活动时刻、两会保障）应委派专人对分局提供现场应急队伍保障服务。
6. 信息安全风险评估服务：分析机房所有信息资产（包括硬件、软件、文档和数据、人力、业务应用、物理环境、组织管理等）的稳定性、可靠性、保密性、可用性、完整性等安全属性，对涉及安全的关键资产进行确认和划控。对资产（包括硬件、业务应用、物理环境、组织管理等）面临哪些潜在威胁，导致威胁的问题所在，威胁发生的可能性有多大等问题进行分析。从技术方面，全面分析系统存在的各种脆弱性，分析弱点被利用的可能性。分析当前系统仍存在的风险并给出相应控制和管理风险的建议。
7. 信息系统加固修复服务：对现有信息安全管理体系中存在的问题进行优化和完善，并协助甲方完成相关文档的编写和宣传；对全网的网络设备和安全设备定期进行修复加固和漏洞扫描，确认主机操作系统、应用系统的安全策略未被更改或还原，查找现有信息安全管理制度与三级等保要求之间的差距。
8. 主要服务设备清单

清单如下，若有遗漏或信息不符，以机房现场内安装设备为准，维保期间新增设备也在维保范围之内，服务商不得以未在下列清单拒绝提供服务。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称及配置摘要** | | **数量** | **备注（维保运维1年）** |
| 1 | 服务器 | 联想X3650 M5（2个六核Intel E5-2620 V3处理器，256 GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 3 | 第三方硬件维保，技术支持运维 |
| 2 | 联想 X3850 X6（2个Intel 八核E7-4820 V2 处理器,128GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 2 |
| 3 | 联想x3650 M5（2个Intel E5-2620 V3 处理器,64GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 1 |
| 4 | IBM X3850（2个Intel 六核E7-4807 V2 处理器,128GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 2 |
| 5 | 联想x3650 M4（2个Intel E5-2620 V3 处理器,64GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 2 |
| 6 | 联想x3650 M4（2个Intel E5-2620 V3 处理器,128GB DDR4内存。3块300G 10K 2.5"SAS硬盘） | 2 |
| 7 | 联想 SR860 （2颗英特尔至强金牌5120 CPU，512 GB DDR4内存。8块1.2T SAS硬盘） | 1 | 技术支持运维 |
| 8 | 存储 | IBM DS5020存储主机 | 2 | 第三方硬件维保，技术支持运维 |
| 9 | IBM DS5020存储硬盘柜 | 2 |
| 10 | 宏杉MS2500存储主机 | 2 |
| 11 | 宏杉MS2500存储硬盘柜（6块480GB SSD硬盘，18块1.8TB 10Krpm SAS ） | 2 |
| 12 | 宏杉MS2500F存储（含硬盘1.8T 25块） | 2 | 技术支持运维 |
| 13 | 华为2200T存储（含硬盘2T 12块） | 1 | 第三方硬件维保，技术支持运维 |
| 14 | 备份硬件 | 鼎甲 DK2000备份一体机（含硬盘4T 12块） | 1 | 第三方硬件维保，技术支持运维 |
| 15 | 酷备R124H 缓存64G，4T硬盘24块 | 1 | 技术支持运维 |
| 16 | 存储网络 | 博科 BR300 24端口交换机，24端口激活，含24个8G短波SFP | 2 | 第三方硬件维保，技术支持运维 |
| 17 | 博科 BR300 24端口交换机，24端口激活，含24个8G短波SFP | 2 |
| 18 | 网络设备 | H3C S5560-54C-EI L3以太网交换机主机,48个10/100/1000BASE-T端口,支持4个10G/1G BASE-X SFP+端口 | 2 | 第三方硬件维保，技术支持运维 |
| 19 | S7703基本引擎交流组合配置(含一体化总装机箱,MCUA主控板\*2,800W交流电源\*2)；3个业务插槽，48端口十兆/百兆/千兆以太网电接口板(FA,RJ45)；24端口百兆/千兆以太网光接口板(SA,SFP)（含24个多模光模块） | 1 |
| 20 | S5720-28P-LI-AC 24个千兆电口，4个上联千兆SFP，单电源 | 1 |
| 21 | H3C S5500V2-54S-EI 48个10/100/1000Base-T以太网端口，4个千兆SFP（含多模模块4个） | 2 |
| 22 | H3C7503 | 1 |
| 23 | H3C 5130 48个10/100/1000Base-T以太网端口，4个SFP+端口 | 8 | 技术支持运维 |
| 24 | 安全设备 | 东软 NISG6K-D4110 防火墙 | 1 | 第三方硬件维保，技术支持运维 |
| 25 | 东软 NDBA7000-S5310数据库审计 | 1 |
| 26 | A10 TH-930 负载均衡设备 | 1 |
| 27 | 网神NSG5500-TY10P防火墙 | 1 |
| 28 | 网神C5000-TG10P运维审计 | 1 |
| 29 | 网神R2000-TG1000P日志审计 | 1 |
| 30 | 网神P5000-TY13P入侵防御系统 | 1 |
| 31 | 绿盟RSASNX3-X 漏洞扫描系统 | 1 |
| 32 | 网神P9000-TG63M 入侵防御系统 | 1 | 技术支持运维 |
| 33 | 铱迅WAF-6000G 应用防火墙 | 1 |
| 34 | 中科富星SNBS-DTP2000数据交换平台 | 1 | 第三方硬件维保，技术支持运维 |
| 35 | 网神隔离网闸 | 1 |
| 36 | 上讯日志审计系统 | 1 | 技术支持运维 |
| 37 | 深信服上网行为管理 | 1 |
| 38 | 网神下一代防火墙NSG5000 | 1 |
| 39 | 深信服VPN设备 | 1 |
| 40 | 其他技术支持 | 备份服务 | 1 | 技术支持运维 |
| 41 | 虚拟化服务 | 1 |
| 42 | 现场服务，日常巡检，技术支持 | 1 |

## 技术服务内容要求

4.1定期巡检

包括网络安全定期巡检以及提供漏洞扫描、攻防演练、风险态势感知分析技术支持等。服务商应指派服务工程师提供每月一次的现场检查服务，并在检查结束后的7日内提供巡检报告给本单位审核确认。预防性检查服务内容应包括但不仅限于以下内容：

1、系统硬件配置检查

服务商应对系统的各项配置(硬件配置、软件配置、核心参数配置、相关的操作系统配置)进行检查，针对不合理配置项提出调整建议，尽可能避免因配置不当造成的系统宕机及数据丢失风险。

2、日志检查

服务商应对系统日常运行日志进行检查并分析错误信息。

3、性能检查

服务商应对系统性能数据（包括系统参数、物理和逻辑分布、资源消耗和竞争等）进行检查，分析潜在的系统瓶颈和可能降低系统性能的因素，提供建议及优化方案，并协助业主完成系统优化实施；

4、安全性检查

服务商应对系统进行定期安全检查以及安全测试，保证系统安全可靠，对发现的问题进行及时补充整改；

5、备份检查

服务商应对存储数据的备份和恢复进行检查和评估（包括系统备份的完整性和可恢复性），针对所存在缺陷，提供可行的解决方案并配合业主实施。

6、维护作业计划

为便于业主在日常维护过程中进行系统运行状况检查，服务商应为业主提供系统日常维护作业计划及维护操作手册，从而保证系统的安全稳定运行。

7、节假日值班服务

国家法定节假日前对系统进行现场巡检，并提供节假日值守名单。

|  |  |
| --- | --- |
| 工作要求 | 1、遵守用户方工作及作息时间安排，服务过程认真负责细致入微；  2、值守人员听从用户方工作人员安排，协调好工作；  3、应急保障时间内需每日填写工作日志；  4、具体事项负责人要求24小时手机开机；  5、各当日应急保障人员要求24小时手机开机；  6、下一班人员到岗后，填写交接单后才能离开现场 |
| 值守人员要求 | 需与用户方办理保密协议，进驻值守；  具有5年及以上信息化及网络安全行业工作经验； |
| 值守时间要求 | 按照用户需求 |

4.2系统升级服务

服务商应提供系统升级服务（包括补丁安装及软件版本升级），并配合业主进行系统升级完成后的测试、提交系统升级实施报告和测试报告等内容。

服务商在系统升级实施前，应向业主提交升级实施方案，明确实施过程、实施时间以及实施中可能出现的问题和风险。

回退机制要求：服务商应承诺严格按照业主批准的实施方案进行补丁安装及软件版本升级的实施。业主可根据业务时限要求或系统运行情况，提出中止安装或升级过程，要求实施回退方案，服务商应在业主要求下保证系统安全回退。

4.3现场维护服务

1、故障处理服务响应时间要求：7×24小时响应

2、对系统故障或与系统相关联的系统故障，服务商在接到业主故障申告电话后，服务商将派工程师在指定的时间内到达现场，并立即进行系统故障诊断、故障排除、系统修复及部件更换等服务，所更换的部件必须为全新原厂商产品或本单位认可的产品（部件费用按市场价收取或由本单位单独采购），直到系统恢复正常运行。

当系统发生重大故障，或影响本单位业务正常运作的故障，服务商应提供备品来替代，如本单位认为有必要服务商技术人员到现场支持时，服务商应按时间要求赶到现场，进行免费维修服务。

3、服务商在系统恢复正常运行后，应对系统进行跟踪，并分析产生故障的原因，7日内提交故障分析报告及解决方案。

4、现场技术服务内容包括：系统故障定位、系统故障修复、系统优化实施

5、现场技术支持服务实施步骤：

现场数据收集--数据分析--合理化建议和实施方案--报告形成；同时根据系统运行情况和业务运行情况制定改进计划并配合实施改进计划，以及实施后对故障系统进行跟踪分析。

4.4热线电话支持服务

1、服务商提供一整套规范的技术支持服务运作体系和流程，稳定的技术服务队伍，提供故障诊断、技术咨询等全方位的技术支持服务。

2、热线电话支持服务响应时间为7×24小时，电话响应时间不超过30分钟。

3、服务商在接受业主热线电话支持服务要求后3日内，应提供相应的技术支持服务报告，得到业主认可确认后表示本次服务完成。

4.5性能优化服务

投标方应指派固定服务工程师负责系统性能优化服务，并在服务后5天内提供详细的性能优化报告。每年的性能优化服务不少于4次。性能优化服务应包括但不仅限于以下内容：

（1）跟踪系统现状。

（2）分析应用类型和用户行为。

（3）评价客户数据库的参数设置、数据分布、硬件和系统资源的使用情况等，并提出相关调整建议。

（4）有效提升系统性能。

4.6应急响应服务

在服务期内，由于紧急断电、病毒、误操作等引起的非系统本身的故障事件，服务商仍应遵照上述条款为用户提供免费服务。

在服务期内，服务商应接受用户对所有事件的响应的要求，同一事件的多次现场响应均计入该事件中，不另行计算。

服务商提供7×24小时全年无休支持服务，接到本单位故障呼叫后，要及时派相关工程师做现场服务，现场服务次数和时间不限；

对于严重故障（影响业主业务正常运作的故障），服务商在接到本单位故障申告后应立即响应，如故障未能在15分钟内通过现场服务工程师或远程支持得到解决，服务商须承诺根据本单位要求派高级服务工程师在1小时内赶到故障现场，提供不间断故障处理服务；

对于一般性故障（不影响业主业务正常运作的故障），如故障未能在30分钟内通过现场服务工程师或远程支持得到解决服务商须承诺根据本单位要求派高级服务工程师在2小时内赶到招标方现场，提供不间断故障处理服务。

4.7清洁保养服务

除尘清洁服务。根据机房的具体情况设定合理的除尘周期。每次巡检对设备吸附尘土情况进行检查，对有必要清洁的设备每季度进行一次清洁；根据实际使用情况，每年两次对设备和机柜进行专业集中彻底的清洁除尘。

4.8技术培训服务

合同期内提供针对性的技术培训，每年不少于1次，培训时间、地点由使用方确定。

4.9本地驻场工程师要求：

中标单位派驻现场专职服务工程师一名，要求在本单位驻点服务。

对驻现场专职服务工程师的管理作如下要求：

1、服从本单位信息中心的统一管理；

2、严格遵守本单位作息时间，工作期间不得从事与工作无关活动；

3、严格遵守本单位的规章制度和保密制度；

4、服务商安排驻点工程师休假期间需补充同等能力熟悉业务的维护人员替补，不得影响本单位工作开展。

5.驻点工程师需拥有出色的学习能力，具备CCNP以上网络能力，能吃苦耐劳，夜间出现系统问题也能第一时间响应，熟悉各类数据库及各类操作系统，逻辑排障能力强，熟练掌握ArcGIS软件，能够分担信息中心日常工作。（驻点工程师需经过本单位面试并且通过，方可签订合同）

6. 驻点工程师工作经验不少于5年。

4.10应急备品备件要求：

应急备品备件指相关设备出现故障后，服务商应及时提供备品备件以恢复本单位网络及系统的正常运行。要求服务商在杭州设立有品种齐全的备件库，保障本单位在发生备件需求时第一时间得到响应。

服务商接到正式通知后，必须在服务等级规定的时限内做出响应，并及时将备件发出。如果最近的备件库没有相同型号的备件，服务商必须以功能相同、性能接近为原则提供备件。如果发生硬件系统停机故障，在接到报修电话后10分钟内响应，并1小时内赶至现场提供维修服务；如果发生硬件系统非停机故障，在接到报修电话后半小时内响应，并根据要求和实际情况到现场提供维护服务；

维修及换件服务：4小时到达现场提供维修及换件服务。

提供整机备件服务：当系统故障，第一次现场服务故障未能排除时，将配备整机备机顶替故障系统运行。

|  |  |  |
| --- | --- | --- |
| 备件类型 | 备机备件 | 数量 |
| 安全类备机 | 奇安信网神智慧防火墙：网络处理能力 8G,并发连接260万，标准配置6个10/100/1000M自适应电口，4个千兆 SFP插槽,2U机架式； | 1 |
| 网络应急备机 | H3C网络交换机：24口千兆交换机，交换容量256G以上，含4个千兆光模块，2个万兆光模块 | 1 |
| 服务器应急备机 | 惠普或联想2U 服务器，配置2颗 E5 六核处理器，300G硬盘2块，256G内存。 | 1 |

中标服务商在中标后2个工作日内，需提供以上备机备件并经用户单位确认之后，方可签订合同。如无法提供或与要求不符的，可认定为虚假应标，取消其中标资格。并重新组织询价。

参与报价的供应商需针对本章节的服务内容要求作出详细的技术响应承诺盖章后并以附件方式上传。否则将视为无效报价。

## 商务要求

本单位拒绝自2018年以来具有劳动纠纷、买卖合同纠纷等不诚信行为的公司或自然人参与投标，一旦查证，取消其中标资格。

中标服务商应在中标后2个工作日内准备完整的资质证明文件递交至采购人处，如发现递交的资质证明文件不符合本次招标所需要提供的资质文件或存在弄虚作假的情况，将上报采购监管部门要求废除中标资格，同时重新询价，并追究相关法律责任。需提交的证明文件如下，缺一不可：

（1）、营业执照（需为杭州本地公司）

（2）、项目组成员（不少于5人）清单及个人简历等证明资料，含在职社保证明（项目组成员不少于3年工作经验，项目经理及驻点人员不少于5年工作经验）。

（3）、项目组工程师证书：CISP证书1份，RHCE证书1份、原厂认证存储工程师1份

（4）、中标服务商具有2019年1月1日至今类似成功案例，提供至少2份合作案例合同，原件备查。

（5）、服务承诺书。

## 付款方式

合同签订后15个工作日内，中标服务商进一步细化目标任务书和维保技术方案，提供相关文档，支付合同总价40%；2021年12月，服务商提交2021年度运维服务总结报告，经本单位确认服务良好、无质量和服务问题后支付合同总价60%。