附件2

卫健局运维服务内容及要求

**一、机房IT设施运维服务**

**（一）机房IT设施运维清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备类型** | **设备型号** | **数量** |
| 1 | PC服务器 | 浪潮 NF8460M3 | 6台 |
| 2 | PC服务器 | Lenovo X3650 M5 | 8台 |
| 3 | PC服务器 | IBM X3650 M4 | 7台 |
| 4 | PC服务器 | DELL R730 | 3台 |
| 5 | PC服务器 | IBM X3650 | 3台 |
| 6 | PC服务器 | IBM X3850 X5 | 2台 |
| 7 | PC服务器 | HP DL385G7 | 1台 |
| 8 | PC服务器 | DELL R710 | 1台 |
| 9 | PC服务器 | DELL R840 | 2台 |
| 10 | 存储 | EMC VNX5300 | 2台 |
| 11 | 存储 | EMC VNXe3200 | 2台 |
| 12 | 存储 | 神州云科NCS4250H | 2台 |
| 13 | 虚拟带库 | 神州云科NDP 320 | 1台 |
| 14 | 存储虚拟网关 | EMC VPLEX | 1台 |
| 15 | 光纤交换机 | 博科300 | 2台 |
| 16 | 光纤交换机 | EMC DS300B | 2台 |
| 17 | 交换机 | H3C S7503E-M | 2台 |
| 18 | 交换机 | H3C LS-5130S-52P-EI | 4台 |
| 19 | 交换机 | H3C S3600V2-28TP | 1台 |
| 20 | 交换机 | H3C S5500 | 1台 |
| 21 | 交换机 | 神州数码DCRS-5960 | 1台 |
| 22 | 交换机 | 华为S5700S-28P-LI | 1台 |
| 23 | 交换机 | H3C S5500V2-48P-SI | 2台 |
| 24 | 交换机 | H3C S5500V3-48P-SI | 2台 |
| 25 | 交换机 | H3C LS-5500-52S | 1台 |
| 26 | 交换机 | 华为S3700 | 1台 |
| 27 | 交换机 | H3C LS-3600V2 | 1台 |
| 28 | 路由器 | H3C S6602-X | 2台 |
| 29 | 防火墙 | 天融信TG-41406 | 2台 |
| 30 | 防火墙 | 天融信 TG-51030 | 2台 |
| 31 | 防火墙 | 360 NSG3000-TE25P-Q | 1台 |
| 32 | 防火墙 | 安恒 DAS-NGFW660 | 1台 |
| 33 | 防火墙 | 天融信 NG-51038 | 1台 |
| 34 | 入侵检测 | 天融信 TI-31114 | 1台 |
| 35 | 防毒墙 | 天融信TU-31513F | 1台 |
| 36 | 网站防护 | 铱讯 WAF-3780 | 1台 |
| 37 | 数据库审计 | 安恒DAS-A1000 | 1台 |
| 38 | 综合日志审计 | 安恒DAS-LOG500 | 1台 |
| 39 | 堡垒机 | 安恒DAS-USM200 | 1台 |
| 40 | 网闸 | 金电网安5000SZ | 2台 |
| 41 | 视频网闸 | 金电网安ZP 3650 | 1台 |
| 42 | 准入管理 | 盈高 ASM6503 | 1套 |
| 43 | 移动准入管理 | 盈高IMC2301 | 1台 |
| 44 | 桌面管理 | 盈高桌面管理 | 1套 |
| 45 | VPN | 深信服VPN-1000-A400 | 1台 |
| 46 | 负载均衡系统 | 深信服AD-1000-D620 | 2台 |
| 47 | 杀毒 | 奇安信网神统一服务器安全管理系统 | 1套 |
| 48 | 杀毒 | 奇安信网神终端安全管理系统 | 1套 |
| 49 | 安全感知系统 | 奇安信网神TSS10000-A58 | 1套 |
| 50 | 流量传感器 | 奇安信网神TSS10000-S53 | 1套 |
| 51 | 数据库实时复制系统 | DSG数据库实时复制系统 | 1套 |
| 52 | 虚拟化平台 | VMware虚拟化软件 | 1套 |
| 53 | 虚拟化平台备份系统 | 卫盟虚拟化平台数据备份系统 | 1套 |
| 54 | 数据库 | Oracle、SQLserver、MySQL、Mongodb数据库日常运维 | 1批 |
| 55 | 城市大脑云资源 | VPC云资源维护 | 1批 |

注：最终运维设备以用户现场实际设备型号、数量为准。

**（二）服务要求**

**1.**要求每年提供不少于1次的备份恢复测试演练和容灾演练服务；运维服务期内提供深信服VPN设备软硬件原厂运维升级服务(2025年11月16日-2026年12月31日），涉及到的费用由中标方承担。

2.按要求落实招标文件中的机房运维要求及整体服务要求。

**二、机房基础设施运维**

**（一）运维设施清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务项目 | 设备型号 | 数量 |
| 1 | 精密空调系统、新风系统维保服务 | 佳力图 13AD12L | 2套 |
| 佳力图 MEAD301 | 1套 |
| 艾默生 DME07MC1 | 1套 |
| 新风机 | 1套 |
| 2 | 不间断电源系统维保服务 | 华为 50KVA | 1套 |
| 先控 30KVA | 1套 |
| 3 | 气体消防系统维保服务 | 灭火系统：新纪元 | 1套 |
| 报警系统：北大青鸟 |
| 4 | 配电、防雷等系统维保服务 | 机房电源：施耐德 | 1套 |
| 5 | 机房环境监控、视频监控系统维保服务 | 环境集中监控系统：赛恩 | 1套 |
| 视频监控系统：海康威视 | 1套 |
| 6 | 机房基础维护 | 门禁系统 | 1套 |
| 除尘清洁、地板、墙面、吊顶、灯管及相关基础配套的维护 | 1套 |

注：最终维保设备以用户现场实际设备型号、数量为准。

**（二）服务要求**

按要求落实招标文件中的机房运维要求及整体服务要求。

**三、网络安全服务**

**（一）服务内容及要求**

**1.网络安全巡查服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | 通过主动扫描、渗透测试等手段，综合检查东阳市卫生健康局的内部网络和外部网络的网络安全责任落实情况。检测网络与信息系统在安全方面存在的安全隐患和安全漏洞，出具网络安全评估检查报告，协助开展网络安全整改工作。检查内容包括，内外网信息系统网络隔离、身份鉴别、访问控制、口令管理、边界防护、数据保护、密码应用、容灾备份、安全审计等技术措施的落实情况和有效性，网络安全监测手段的建设和运行情况，相关软硬件和业务系统是否存在技术漏洞、业务逻辑漏洞；是否关闭或删除了不必要的系统、网站、应用、服务、端口和链接；是否存在重要漏洞未修复情况，是否存在弱口令、默认口令、通用口令和长期未更换的口令等。 |
| 服务要求 | 1.投标人应保证业主方信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对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，帮助业主方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。  2.投标人应在得到业主方授权后方可开始实施相关检查评估工作。  3.投标人应确保实施检查评分的服务人员的工作保密性，签署相关的保密协议，在未经业主方允许的情况下，不得将识别的漏洞外泄、传递。  4.实施检查评估服务后，未经业主方同意，禁止在系统留存后门。  5.检查评估中涉及的工具均由投标人自行提供。 |
| 服务频率 | 每季度1次 |
| 服务交付 | 《网络安全检查评估报告》等 |

**2.专项网络安全检查服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | 针对东阳市卫生健康局网络及重点信息系统开展专项网络安全风险排查工作，确保网络安全风险隐患及时排除。 |
| 服务要求 | 1.投标人应保证业主方信息系统正常运行前提下，通过远程或本地方式对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，协助业主方理清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，切实保证信息系统网络安全。  2.投标人应确保实施人员的工作保密性，签署相关的保密协议，在未经业主方允许的情况下，不得将识别的漏洞外泄、传递。  3.实施服务后，未经业主方同意，禁止在系统留存后门。  4.检查中涉及的工具均由投标人自行提供。 |
| 服务频率 | 按需 |
| 服务交付 | 《网络安全专项检查报告》等 |

**3.CNVD漏洞数据报送服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | 基于国家信息安全漏洞共享平台（CNVD），收集、分析涉及用户的安全漏洞，在发现涉及用户相关信息系统安全漏洞后，第一时间向用户报送，并向用户提供技术咨询服务，协助排除风险隐患。 |
| 服务要求 | 漏洞报送涉及信息系统类型包括网站、APP、信息系统等。漏洞报送内容包括漏洞事件名称、漏洞引发的威胁、评分评级、影响产品、信息来源、漏洞描述、影响范围、漏洞验证情况、发现时间等。 |
| 服务频率 | 不定期推送 |
| 服务交付 | 《CNVD漏洞报告》 |

**4.应急响应服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | 1. 投标人应在业主方遇到重大或突发事件后按照要求的服务响应级别采取相关的措施和行动。帮助业主方正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态。   2、本次采购的应急响应包含但不限于以下几类安全事件：   * WEB 安全事件   针对 B/S 类信息系统或网站遭受恶意入侵，利用网站进行反动信息、赌博、黄色等信息发布，传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括但不限于：篡改、暗链、挂马、Webshell 等。   * 恶意程序事件   针对遭受的各类恶意程序事件进行快速处置，包括不限于病毒事件/木马事件、蠕虫事件、僵尸网络事件、勒索病毒事件、挖矿病毒事件等。   * 网络攻击事件   针对业主方由于信息系统的配置缺陷、协议缺陷、程序缺陷，造成的信息系统异常的安全事件进行应急响应。   * 信息破坏事件   针对业主方信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件进行应急响应，包括但不限于系统配置遭篡改、数据库内容篡改、网站内容篡改事件、信息数据泄露事件等。 |
| 响应时间要求 | 1. 投标人应提供 7×24 应急响应服务。要求服务方工程师队伍需要启动紧急响应流程，第一时间调派工程师到达用户现场，制定解决方案，并协助处理，确保系统尽快恢复正常运行。对于同一故障，紧急响应的服务次数和服务时间不作限制。服务方的技术人员需要跟进到问题解决为止。   2、安全事件要求应急团队须在 5 分钟内，对信息安全事件做出响应，并严格按照业主方信息安全等级要求迅速到达现场并解决问题：   * 特别重大事件（Ⅰ级），5 分钟作出响应，提供远程 7×24小时响应服务、1 小时到达现场进行应急响应服务。 * 重大事件（Ⅱ级），10 分钟作出响应，提供远程 7×24 小时响应服务、2 小时到达现场进行应急响应服务。 * 较大突发事件（Ⅲ级），30 分钟作出响应，提供远程 7×24小时响应服务、4 小时到达现场进行应急响应服务。 * 一般性突发事件（Ⅳ级），30 分钟作出响应，提供远程 7×24小时响应服务、远程无法解决时，在 4 小时到达现场进行应急响应服务。   3、每次故障处理完毕3个工作日内提供详细的故障处理报告。 |
| 服务频率 | 按需 |
| 服务交付 | 《XX 系统（事件）应急响应报告》 |

**5.网络安全培训服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | 根据用户需求开展针对性网络与信息安全培训，提高用户隐私保护、常规攻击防护、信息安全管理等能力，增强用户网络安全防护意识，规避网络攻击风险，补齐短板、夯实基础。 |
| 服务要求 | 聘请业内专家讲师为用户提供网络安全综合性培训。针对管理和技术两个层面制定网络安全培训计划，通过安全培训使相关人员的安全意识、安全技术能力及安全管理能力有明显提升。 |
| 服务频率 | 每年不少于1次 |
| 服务交付 | 《网络安全培训课件》等。 |

**四、数据库运维服务**

**（一）服务内容**

运维服务清单如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **数量** |
| 1 | 核心数据库运维 | 2套 |
| 2 | 数据库可视化运维监控系统运维 | 1套 |
| 3 | 数据库安全审计系统运维 | 1套 |
| 4 | 运维一体机软硬件运维 | 1套 |

**（二）服务要求**

1.预防性巡检服务

定期提供全面巡检服务，巡检范围为运维服务清单内所有运维硬件及软件，及时发现各种隐患，并做出相应处理。要求每季度提供不少于1次的上门巡检和维护服务，出具详细的巡检报告，并给出优化解决方案。

运维服务期内提供美创数据库可视化运维监控系统、美创数据库安全审计系统和运维一体机软硬件(硬件：OKPT-G300、软件：美创自动化运维平台)原厂运维升级服务(2025年8月10日-2026年12月31日），涉及到的费用由中标方承担。

2.灾难性故障紧急服务

在整个服务期内，如果发生对业务产生重大影响的数据库层面问题，要求服务方工程师队伍需要启动紧急响应流程，第一时间调派工程师到达用户现场，确保系统尽快恢复。对于同一故障，紧急响应的服务次数和服务时间不作限制。服务方的技术人员需要跟进到问题解决为止。

当技术或设备能力不能满足业主方维保需要，对关键性问题若2小时内无法修复或对一般问题12小时内无法修复的，业主方有权请任何第三方公司进行维保，由此产生的一切费用，由中标方承担。

3.数据灾难挽救服务

在极端情况下，如备份丢失或者备份比较久远，需服务方专业技术人员最大限度找回需要的数据，降低数据丢失损失。

除利用数据库自身具备以及用户提供的各种技术实现数据灾难挽救外，同时还能提供一个自行开发的数据挖掘工具，该工具能支持在数据库无法打开的情形下，实现数据最大可能的IO读取，获取数据表格。

4.数据库性能优化服务

系统运行情况与应用业务紧密相关，系统运行效率直接影响到应用业务的处理能力和前台应用的体验。运维人员应根据对目标系统的了解和检查情况，结合实际应用系统及主机网络运行环境，制定数据库性能调优方案，对数据库提供性能评测、瓶颈分析、优化提升建议，并与系统开发商一起协同配合，解决系统中的性能重疾与隐患。每年提供不少于1次的数据库性能优化服务。

5.数据库安装升级迁移服务

根据业主方的实际情况，制定数据库安装、升级、迁移实施工作计划，并配合用户进行实施工作。

6.数据库备份恢复演练服务

根据实际应用角度出发，根据硬件环境，应用类型进行分析，推荐多种数据库备份策略以及实施，为业主方系统数据库提供最安全可靠的备份服务，同时为了备份的有效性，定期对备份进行模拟恢复的操作以验证备份的有效性时效性，确保在紧急情况在最快的时间内恢复数据保证生产数据库的运行。每年提供不少于1次的备份恢复测试演练服务和容灾演练服务。

7.技术培训及咨询服务

提供技术培训服务，帮助用户提高技术水平和解决常见故障的能力。为业主方数据库的运行、数据安全建设等提供技术咨询，根据实际情况，结合有关安全要求，提出调整建议。

**五、软件运维服务要求**

**（一）服务要求**

1.日常运行维护

提供7×24小时热线或远程技术支持服务，及时处理和解答问题。做好日常运行维护工作和操作使用指导。

（1）包含软件问题排查、修改程序本身问题、版本升级、功能完善与升级、用户需求修改、各类第三方系统接口问题处理、各类统计报表及数据准确性维护、在用户允许下的后台数据查询、提供配合其他系统的相关的数据接口、针对信息安全等级保护整改要求修改等工作，保证系统正常运转。对于错误性、程序本身的Bug并影响业务流程的需求，应立即响应(时间不能超过3个工作日)。

（2）定期更新《常见问题处理手册》并提交给用户，用户在使用系统时出现问题，可通过手册查询解决方案，帮助医院管理员提高维护水平并能快速的解決常见问题。

（3）定期收集相关用户的需求，并将需求归纳后形成文档，根据这些需求对系统进行更新，以不断完善该系统。

2.故障修复服务

提供7×24小时故障修复响应服务，对用户反映的紧急故障问题，应在10分钟之内做出实质性响应，第一时间排除故障，确保系统的正常高效运行。如远程无法解决问题，则要求及时派相关认证工程师到达现场，提供不间断故障处理服务，直至故障解除，现场服务次数和时间不限。

当技术或备件能力不能满足业主方维保需要，对关键性问题若2小时内无法修复或对一般问题12小时内无法修复的，业主方有权请任何第三方公司进行维保，由此产生的一切费用，由中标方承担。

若本项目的软硬件系统发生重大故障，须在故障发生的第3个工作日内提供故障分析报告，并提出问题解决方案。

3.预防性巡检

定期对系统进行全面检测，确认系统运行状态，检查系统错误记录，排除隐患故障，并进行系统运维工作及提出预防措施。每季度提供不少于1次的现场巡检和维护服务，并出具详细的巡检报告。

4.数据维护与上传（若无涉及，此项不做要求）

（1）日常相关数据处理：对卫生健康局提出的相关数据的处理，并针对提出的问题进行后台数据的完善，以及数据的核查、导出等维护工作。

（2）根据实际的业务需求，拓展完善相关数据集，对东阳市数据传输规范进行相应的调整或扩展。

（3）平台数据上传：根据金华市平台数据采集交换技术规范的要求，做好数据对接，并根据金华市平台规范的调整或扩展，对东阳市数据传输规范进行相应的调整或扩展，实现与金华市平台的互联互通，且数据质量达标。数据质量连续不达标情况下，中标方须在3个工作日内完成问题整改。如若整改情况依旧达不到标准的，需到场集中办公完成问题整改。

（4）维护外部数据接口，保障接口的畅通以及在更改或新增接口时，进行接口规范的变更或增加，支持与第三方数据接口的对接工作。

（5）数据监测：主要监测数据的规范（准确）性、完整性、一致性和及时性。

5.数据保护及性能调优

对数据库进行日常性能巡检及调优，保障整体性能。配合做好数据备份和数据恢复测试，协助进行灾难恢复、数据安全性评估、灾难事件分析。

6.技术咨询及培训服务

提供软件使用问题解答、软件使用指导、软件功能介绍、技术咨询等服务。提供用户培训服务，在项目维护期内对业主方技术人员提供必要的技术培训，包括数据结构培训、软件设计培训、软件应用培训等；对业主方提供必要的用户操作培训等现场服务。

7.电话投诉与回访服务

在系统运维服务期间，如对服务质量和服务人员不满意，可以进行投诉，并在第二个工作日内向用户答复投诉处理情况；在项目运维期间，不定期对某次服务进行电话回访，了解服务完成的情况和质量。

8.值班保障要求

提供节假日专人值班服务，确保在节假日如遇到问题能够及时找到专人解决，保证系统的稳定运行。按要求完成节前巡检。

9.其他要求

（1）中标应方须保证本项目人员的稳定性，在未经业主方同意，不得单方面擅自更换项目组人员。

（2）运维人员在故障处理、性能优化、系统更新等过程中，必须按照业主方内部的管理流程，对设备的硬件配置及软件配置参数的变更进行评估、审批后方可实施，并及时记录变更实施过程。不得擅自对业主方业务经营数据进行增删、修改等操作。

（3）如业主方需在本合同所维护的内容上迁移其应用软件及其它软硬件产品，投标人应承诺无条件配合完成安装工作。

（4）中标方对系统或运行环境等进行改动后，须及时向业主方递交最新的文档资料，该文档资料作为验收资料的一部分。