**附件：**

**说明：**本技术要求仅做参考，不是唯一指标。

**数据库及网络安全服务需求**

**运维服务内容要求如下：**

|  |  |  |
| --- | --- | --- |
| **服务名称** | **服务内容** | **数量** |
| 数据库运维服务 |  HIS 系统、电子病历系统、SAP ERP 系统、移动护理系统、手麻系统共5套生产库，及所有系统的备份库和容灾库 | 2年 |
| 等级保护测评服务 | HIS、电子病历平台、互联网医院信息系统、互联网医疗服务监管平台 | 4套系统 |
| 安全运维服务 | 为医院全网提供安全运维服务，提供定期安全评估和安全检查，及时修复潜在安全漏洞，保障医院信息化安全、稳定运行。 | 1年 |

1. 本期服务详细内容和要求
	1. 数据库运维服务
* **数据库运维范围**

|  |  |  |
| --- | --- | --- |
| 数据库名称 | 应用系统 | 操作系统 |
| Oracle 11g 数据库 RAC | HIS系统 | Linux |
| Oracle 11g 数据库 RAC | 电子病历系统 | Linux |
| Oracle 10g 数据库 单机 | SAP ERP系统 | Windows |
| Oracle 11g 数据库 RAC | 移动护理 | Linux |
| Oracle 11g 数据库 RAC | 手麻系统 | Linux |
| 数据库备份系统 | HIS系统 | Linux |
| 电子病历系统 | Linux |
| 移动护理 | Linux |
| SAP ERP系统 | Windows |
| 手麻系统 | Linux |
| 数据库容灾系统 | HIS系统 | Linux |
| 电子病历系统 | Linux |
| 移动护理 | Linux |

* **数据库维护支持服务要求**

|  |  |
| --- | --- |
| **维护项目** | **内容要求** |
| **基本服务要求** |
| 电话支持服务 | 全年7×24小时电话支持 |
| 邮件支持 | 有，提供工作日邮件支持，第二个工作日内回复 |
| 远程支持 | 提供远程操作支持和远程拨入支持 |
| 现场支持 | 根据客户需求，工程师提供现场服务，例如：定期巡检、数据库配置调整等服务 |
| **数据库服务要求** |
| 数据库规划 | 有，提供数据库规划 |
| 日常管理规范制定 | 有，协助客户制定数据库日常管理规范 |
| 补丁服务 | 根据客户需求服务期内进行现场打补丁服务 |
| 数据库性能调优 | 根据客户需求服务期内提供 |
| 数据库日常维护（解决巡检发现的数据库问题） | 根据客户需求服务期内提供 |
| 数据库健康检查周期 | 至少每季度1次 |
| 数据库SQL、表空间、日志、告警事件处理 | 根据客户需求服务期内提供 |
| 紧急响应次数 | 服务期内不限次数紧急响应 |
| 备份与恢复方案 | 制订、协助实施数据库备份与恢复方案 |
| 数据库灾难恢复演练 | 根据客户要求提供灾难恢复演练服务 |
| 数据库维护手册 | 提供定制的数据库维护手册 |

* **数据库服务内容说明**
	+ 电话支持服务

拥有热线电话服务系统，能提供7×24小时不间断的电话支持服务。

* + 紧急故障处理服务

投标人必须提供400电话和项目经理电话，保证在用户系统出现重大事故时多路径、多渠道救援服务，保证用户系统安全稳定运行。

保证在接到紧急故障电话后15分钟内响应，2小时内到达现场，并必须连续进行维修，直到正常运行。

* + 请求式专家现场支持服务

可提供服务期内的数据库专家现场技术服务，内容包括：数据库安装帮助；数据库的重新规划；现场问题的诊断及分析；实施问题的解决方案；数据库性能调整等。

* + 数据库备份与恢复

提供数据库的备份与恢复的方案设计、操作培训和具体实施。数据库在线备份和恢复解决方案是采用专业数据库备份软件完成数据库的在线备份和恢复，满足系统自动、快速的备份和恢复要求，使得数据库系统能更好的满足7×24小时的业务要求。

具体内容如下：

系统数据在线数据备份和恢复规划；

系统数据在线数据备份和恢复方案的实施；

系统数据在线数据备份和恢复方案的测试；

系统数据备份和恢复方案的培训；

* + 数据库灾难恢复演练

提供数据库的容灾数据库灾难恢复演练服务，包括：

制定容灾数据库灾难恢复演练实施文档；

定期协助客户共同实施灾难恢复演练；

对灾难恢复演练进行总结，为下次演练做好准备。

定期的数据库灾难恢复演练可以帮助用户更熟悉容灾系统的运作机制，在真正灾难出现的时候能熟练快速启动容灾系统顶替业务上线，减少生产系统的下线时间。

* + 数据库性能调整服务

此服务指对用户的数据库进行性能方面的分析、评估、检测、调整、测试，以提高数据库系统的整体性能。

具体内容如下：

对数据库信息进行收集；

查找引起数据库性能下降的各种原因，制订解决方案；

根据业务特点及数据库状态，制定数据库调优方案；

在业务允许的情况下，对系统做好备份准备；

在业务允许的情况下，调整数据库；

测试数据库，保证数据库的可用性；

协助测试应用软件，检测调优的有效性。

* + 数据库补丁包服务

此服务主要完成数据库增打补丁的需求，使打完补丁后的数据库环境能够正常运作，发挥数据库软件应有的功能。定期提供所发布的相关软件更新和补丁情况，及时通知影响系统安全运行的软件漏洞和修补方法，并提供相应的现场服务。

* + 远程操作或远程拨号诊断

可对部分数据库问题提供远程操作或远程拨号诊断服务。以加快问题确诊的速度，减少故障时间。

* + 数据库健康检查周期（巡检服务）

定期到现场进行系统巡检。并提交相应的数据库巡检报告，报告内容主要包括数据库基本信息、当前配置对稳定性的影响、当前系统的性能评估。对可能会产生其他一些影响的问题，或者优化方案需要增加某项资源(例如性能瓶颈可能是缺乏内存或CPU资源)，必须在提交的报告中详细描述问题的成因，影响范围，建议的解决方案，以及解决问题的风险。

* + 现场培训服务

提供现场的培训服务，内容为与维护数据库相关的管理和维护课程。

* + 定制数据库维护手册

总结归纳数据库现有系统和应用特点，制订相关的数据库日常管理方式、数据库定期性能检查内容和方法、制订描述手册内容和使用方法并针对性的进行数据库管理培训服务。帮助建立数据库信息系统的维护规定，对业务系统的稳定运行得到可靠保证。提升数据库维护人员的数据库管理水平和能力，使数据库管理员具备定期检查能力，保障数据库系统的正常工作，防患于未然。

* + ▲数据库自动化监控要求

在服务期内，免费为医院提供一套数据库自动化监控软件，辅助医院数据库运维工作，能实时监控数据库运行重要指标，如：

数据库服务器资源使用情况（CPU、内存等）

数据库存储磁盘组使用情况

数据库表空间使用情况

数据库日志的最新告警信息

数据库连接数等

数据库自动化监控软件提供和医院的短信平台、微信公众号接口的能力，在医院提出需求的时候，能将告警信息通过以上途径及时推送，以保障故障和隐患的及时发现和处置。

* + 服务期限要求

签订合同当日起开始计算为“维护系统清单”内的数据库提供1年的保修维护服务。

**等级保护测评服务**

按照国家和行业的要求，医院信息系统要定期进行等保测评初审和复审，以确认医院信息系统的安全配置是符合国家等级保护标准的要求。在本期服务中，中标人要提供医院本年度等保的全生命周期的服务，提供从等保备案、差距测评、整改指导、等保验收、备案回执等所有等保阶段的服务。本期医院需要通过等保的系统和通过等保的级别如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **定级情况** | **机房位置** |
| 1 | HIS系统 | 三级 | 本单位机房 |
| 2 | 电子病历平台 | 三级 |
| 3 | 互联网医院信息系统 | 三级 |
| 4 | 互联网医疗服务监管平台 | 三级 | 广东省政务云机房 |

* **等保测评服务要求**

▲本项目包含等保测评和等保验收的费用，中标公司完成测评后并且院方整改完成后，由中标方聘请具有验收资质的专业公司对测评的系统进行验收，最终通过互联网线上提交审核通过后、现场将单位情况表、信息系统备案表、信息系统定级报告和其他相关资料提交至广东省公安厅网警总队进行备案。

▲协助编写如下文档内容：

《单位情况表》；

《信息系统备案表》，共计4份；

《信息系统等级保护定级报告》，共计4份；

其他资料如网络拓扑图、安全管理制度等。

▲最终获取广东省公安厅网警总队提供的《信息系统安全等级保护备案证明》。

中标方须对客户信息系统安全按照上表的等级保护级别状况进行测评，包括几个方面的内容：

1、安全技术测评，主要包括：物理安全技术测评、网络安全技术测评、主机安全技术测评、应用安全技术测评、数据安全与备份恢复技术测评等五个层面上的测评；

2、安全管理测评，主要包括：安全管理机构测评、人员安全管理测评、系统建设管理测评、系统运维管理测评等四个层面上的测评；

3、系统整体测评，主要包括：安全控制间安全测评、层面间安全测评、区域间安全测评、系统结构安全测评等四个层面上的测评

在客户等级保护测评项目的测评过程中，必须遵循和贯彻信息技术的国际、国内标准，制定一系列满足信息网络和应用系统正常运行的管理规程。

设计依据及参考规范如下：

 GB17859-1999计算机信息系统安全保护等级划分准则

《信息安全技术网络安全等级保护基本要求》（GB∕T 22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB∕T 28448-2019）

 GB/T22240—2008信息系统安全等级保护定级指南

 信息系统安全等级保护测评过程指南（国标报批稿）

 信息系统安全等级保护测评要求（国标报批稿）

 国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）

 2004年9月四部委局联合签发的《关于信息安全等级保护工作的实施意见》

 《广东省深化信息安全等级保护工作方案》(粤公通字[2010]45号)

 《计算机信息系统安全等级保护管理要求》

 《计算机信息系统安全等级保护通用技术要求》

* **服务工具要求**

本项目在实施过程中所使用到的专业安全服务工具，投标人必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性，由此产生的一切责任由投标方负完全责任。

* **服务人员要求**

**▲**投标方参与本项目的人员至少有3人，项目经理必须具有工业和信息化部计算机信息系统集成资质认证工作办公室颁发的高级项目经理证书、测评工程师具有中国信息安全测评中心颁发的注册信息安全专业人员证书（即CISP证书）资质证书，配合测试的工程师具有其他相关资质，如OCP、VCP、HCNP等。

**安全运维服务**

1. * 定期安全检查

**服务频次：每季度一次**

**服务内容：**

对医院的现网整体安全提供全面的巡检服务，巡检的内容包括但不限于：

1. 安全设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备标签完善程度；
2. 安全设备软件版本信息、当前IOS版本信息、最新IOS版本信息、设备持续运行时间、设备IOS备份情况、设备CPU利用率、设备内存利用率、设备模块运行状态、设备风扇及电源状况、设备端口数量、设备端口类别、设备端口类型、设备运行机箱温度；
3. 安全设备连通性、冗余协议运行状态、VLAN信息、设备配置信息分析、多余配置信息分析、配置精简建议、IOS安全建议、防火墙信息、防火墙策略、防火墙DMZ区检查；
4. 对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估；
5. 对安全系统瓶颈和资源竞争情况进行分析，找出潜在问题。
6. 对服务器、终端做周期检查，主要内容是检查是否存在高危漏洞，杀毒软件病毒库是否最新。
	* 架构改动安全风险评估

**服务频次：一年内不限次数**

**服务内容：**

在现网架构改动、新系统上线、配置变更的时候，对变动带来的风险进行识别和评估，提出风险预防和必要的整改措施。风险评估的内容包括但不限于以下内容：

1. 存储被测系统重要数据的介质的存放环境；
2. 整个系统的网络拓扑结构；
3. 安全设备，包括防火墙、入侵检测设备、防病毒网关等；
4. 边界网络设备，包括路由器、防火墙和认证网关等；
5. 对整个信息系统或其局部的安全性起决定作用的网络互联设备，如核心交换机、汇聚层交换机、核心路由器等；
6. 涉及到信息系统安全的所有管理制度和记录。

风险评估的方式包括人工访谈、工具检测、登录系统检测、文档分析、渗透测试等。

* + 安全事件紧急响应

**服务频次：一年内不限次数**

**服务内容：**

安全事件响应要求服务商在广州有总公司、分公司或办事处常驻有安全工程师，在接到医院的安全事件紧急救援服务请求后，本地安全工程师立即响应，通过预先确认的远程连接方式登录到相应的系统上，对安全事件进行排查，在发现远程登录无法解决的安全事件后，立即采用最快的交通方式赶赴医院现场，2小时内可达到医院的现场。

当医院发生大规模的安全事件后，如信息系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、黑客攻击、蠕虫或大面积爆发病毒等，服务商常驻广州的安全团队将在2小时之内赶赴现场协助解决问题，必要时应提供入侵调查分析、安全审计预警与黑客追踪服务。

应急响应服务包括远程应急响应服务和本地应急响应服务，响应的主要内容如下：

1. 消除潜在安全隐患： 通过日志信息和其他必要信息，检查后门程序和网络系统漏洞，消除其再次受到攻击的可能性，即消除今后的安全隐患，对系统的安全进行重新评估。
2. 检查安全日志： 通过检查系统、防火墙、路由器等系统安全日志，为确认攻击来源和攻击手段以及调查取证提供必要的条件。
3. 主机恢复： 在信息系统网络或主机受到攻击并且出现网页遭替换或系统丢失等恶性事件后，确认已经消除安全隐患，在系统网络管理人员的协助下，对应用系统或操作系统进行恢复，保证系统资源在第一时间内的可使用性。
4. 网络恢复： 医院信息系统的核心交换机、路由设备等网络设备出现问题，在确定是受到攻击所造成的情况下，确认已消除安全隐患，在经过医院授权后，对网络设备进行恢复，保证医院信息系统网络资源在第一时间内的可使用性。
	* 安全配置备份

**服务频次：不定期备份，一个季度一次**

**服务内容：**

1. 为了保证安全设备的健康运行情况，使得设备在失效或配置丢失时，能依靠备份尽快地恢复系统与配置，保护关键策略，保证配置不丢失，特制定本服务。
2. 关键的网络安全设备的策略配置进行备份，防止策略的丢失与错误变更配置；涉及备份和恢复的事由专人负责备份工作，并认真填写备份日志。
3. 备份数据应该严格管理，妥善保存；备份资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。
4. 一旦发生配置丢失或数据破坏等情况，要由负责人员进行备份数据的恢复，以免造成不必要的麻烦或更大的损失。
	* 安全设备日志分析

**服务频次：一季度一次**

**服务内容：**

1. 日志收集：定期统一收集各个安全设备的日志和报表进行存档以便分析。
2. 分析日志：根据甲方设备的具体情况，分析关键服务器、安全设备等设备的日志, 采取人工加工具的审计分析方法对日志信息进行综合分析,找到当前的系统及网络设备中存在的隐患和被攻击痕迹。
3. 生成报告：根据以上评估，生成具体的日志分析报告，为甲方量身定制出专业又极具可读性的报告，并会针对报告中的各项问题，为甲方提供修补建议，使发现的问题能尽可能早的得到解决，避免引起更大范围的影响和损失。
	* 安全建设配合响应

**服务频次：一年内不限次数**

**服务内容：**

在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全技术人员指导配合进行安全相关工作，工作内容包括但不限于以下内容：

医院网站漏洞排查；

公安部门递送的安全检查或安全漏洞通知；

上级部门递送的安全检查或安全漏洞通知；

国家重大事件的安全保障检查；

突发性事件的检查通知或现场检查；

在上述事件发生的时候，医院需要有安全水平高的行业技术人员配合医院开展安全方面相关工作，乙方要根据约定的时间安排专业安全工程师提供远程或上门的安全相关服务，具体服务内容由医院和乙方根据具体要求商议决定。

* + 安全设备配置适应性调整

**服务频次：一年内不限次数**

**服务内容：**

在相关安全设备配置需要调整时，如：安全策略调整、新链路配置、产品参数调整等；乙方必须派遣工程师进行配置风险评估、提出调整方案并实施。安全相关设备配置包括但不限于以下情况：

网络出口新增加，评估新网络出口的风险和安全防护措施；

防火墙、UTM等边界类设备的配置变更，详细记录变更内容，包括IP策略、端口策略、放通/禁止策略等；

入侵防御、网络行为分析等旁路安全设备配置变更，包括协议监控、端口监控、联动策略等；

杀毒软件、准入控制等终端管理类软件的配置变更，包括扫描策略、准入方式、控制范围等；

乙方在协助医院进行安全设备或软件的配置变更时，要充分考虑到配置变更过程中和变更后带来的安全风险，采取一定的预防措施，将风险降低到最小，最小化对医院正常业务开展的带来的影响。

* + 系统漏洞扫描与分析

**服务频次：每季度一次**

**服务内容：**

乙方定期利用专业的技术工具对系统进行测试，包括基于网络探测和基于主机检测的漏洞扫描、数据库漏洞扫描等，扫描相关使用的专业工具版本由乙方提供，医院无需为该工具支持额外费用。

乙方对服务器主机、业务终端设备发现的问题或安全漏洞提出整改建议，并协助甲方做好整改工作。包括服务器高危漏洞在不影响业务的情况下协商修复；终端健康情况检查。

* + 主机基线检查

**服务频次：一年轮询检查250个IP，每个检查一次**

**服务内容：**

安全基线是保持信息系统安全性、机密性、可用性的最小安全控制，是系统最小安全保证，是最基本的安全要求。

安全配置检查:系统管理和维护的正常配置，合理配置，及优化配置。配置检查主要针对操作系统、网络设备、安全设备、数据库等，检查项包括系统目录权限，帐号管理策略，文件系统配置，进程通信管理等方面。

安全机制检查:安全机制的使用和正常配置，合理配置，及优化配置。例如日志及审计、备份与恢复，加密与通信，特殊授权及访问控制等安全特性。

* + 安全加固

**服务频次：根据250个IP漏洞扫描结果和主机基线检查，修复高危漏洞和配置主机基线**

**服务内容：**

安全加固对象是漏洞扫描和基线核查中发现的问题，包括网络设备、安全设备、主机操作系统、中间件、数据库。安全整改加固建议主要关注帐号口令、访问控制、设备防护、安全审计等问题。

账号口令：管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

访问控制：应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

安全审计：应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

设备防护：应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

漏洞修复：当发现高危紧急的漏洞时，提供漏洞分析和加固建议，及时对操作系统进行加固，并协助应用厂商修复应用中间件的漏洞。

* + 渗透服务

**服务频次：一年一次，3个核心系统**

**服务内容：**

渗透测试主要是模拟黑客的攻击方法，检测网站、网络协议、网络服务、网络设备、应用系统等各种信息资产所存在的安全隐患和漏洞。

渗透测试主要分为扫描和人工两部分，依靠带有安全漏洞知识库的网络安全扫描工具以及安全专家对漏洞的深入了解，其特点是能对被评估目标进行覆盖面广泛而且更深度的安全漏洞查找，并且评估环境与被评估对象在线运行的环境完全一致，较真实地反映网站及服务器系统、网络设备、应用系统所存在的安全问题和面临的安全威胁。

* + 应急演练

**服务频次：一年一次**

**服务内容：**

定信息系统的应急预案，定期举行应急演练,应急响应处置，及时发现安全问，准确分析和查找产生问题的原因，针对问题制定整改工作方案，落实整改措施，并提供具体实施的技术服务，逐步建立一套完整的信息安全防护体系，可实现对未知威胁有检测能力、非法攻击行为有分析阻断能力、信息系统弱点有探测能力及安全事件有持续监控能力。

* + 安全培训服务

**服务频次：一年一次**

**服务内容：**

配合医院展开安全建设和运维的工作，定期对医院信息科相关人员提供信息安全技术培训，提升医院信息安全意识和技术知识水平。

培训对象

医院系统管理员、网络管理员、数据库管理员、安全审计员等专业技术人员。

培训内容包括但不限于以下内容：国家等级保护流程与相关内容、医疗行业等级保护建设案例分享、医疗行业网站建设和漏洞防范介绍

* + 安全制度建设

**服务频次：一年一次**

**服务内容：**

结合甲方信息安全的实际情况，为甲方提供信息安全制度建设服务，服务内容包括但不限定于：

网络安全工作总体方针和安全策略

安全管理组织规范

外部人员访问管理制度

移动存储设备的使用管理制度

安全事件报告和处置制度

恶意代码防范管理制度。

* + ★服务期限要求

签订合同当日起开始计算为医院全网提供1年的安全运维服务。

 信息科

 2020年6月19日