**数据库系统与网络安全服务**

**技术需求书**

**一、项目服务内容**

|  |  |
| --- | --- |
| 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电话拨入支持 |
| 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、故障配件更换、数据库配置变更等服务 |
| Oracle**数据库服务要求** |
| Oracle数据库配置变更 | 根据客户需求服务期内提供 |
| Oracle数据库升级服务 | 根据客户需求服务期内提供 |
| Oracle数据库故障排查 | 根据客户需求服务期内提供 |
| Oracle数据库定期巡检 | 每个月巡检一次 |
| Oracle数据库日常维护和迁移服务 | 根据客户需求服务期内提供 |
| Oracle数据库性能调整 | 根据客户需求服务期内提供 |
| Oracle数据库补丁实施 | 根据客户需求服务期内提供 |
| Oracle数据库告警事件处理 | 根据客户需求服务期内提供 |
| Oracle数据库紧急响应 | 根据客户需求服务期内提供，服务期内不限响应次数 |
| Oracle数据库备份系统维护 | 根据客户需求服务期内提供 |
| Oracle DG日常维护和迁移服务 | 根据客户需求服务期内提供 |
| Oracle DG数据库定期巡检 | 至少每月1次，和数据库健康检查周期保持一致 |
| Oracle DG故障排查 | 根据客户需求服务期内提供 |
| Oracle DG容灾演练 | 根据客户需求服务期内提供 |
| **安全与运维服务** |
| 安全漏洞扫描服务 | 对全院所有系统进行漏洞扫描评估，及时发现系统中存在的安全漏洞，出具漏洞扫描评估报告和加固报告及协助修复实施。可根据实际情况如重大活动前或敏感时段保障项目前增加安全扫描服务。 | 1年4次 |
| 渗透测试服务 | 通过模拟黑客攻击对医院目标系统进行渗透测试，发现分析并验证其存在的安全漏洞并提供安全加固报告及协助修复实施。 | 1年4次 |
| 安全加固 | 对全院网络设备、安全产品、操作系统、应用系统、数据库、虚拟化、常见中间件及安全基线相关的应用等信息资产的安全配置策略和漏洞实施必要的安全加固整改。针对使用技术检测手段及等级保护测评发现的安全问题，协助对医院存在安全问题的对象进行实施加固整改工作。 | 全年 |
| ▲人员驻场运维 | 采用驻场机动混合的整体服务模式，驻场人员提供5\*8小时的现场服务，提供所有技术支持、安全设备巡检、新系统上线安全评估、漏洞补丁修复、安全服务请求、安全服务工作日常处理、跟进；安全故障处理的单点专员联系，每月向医院提供安全情况报告。 | 1人 |
| 安全巡检服务 | 配合用户对信息安全管理及安全技术进行检查，包括安全管理制度及执行情况、防病毒系统的版本与升级情况、安全合规情况、安全设备的系统性能情况，系统开放服务及安全策略检查，优化。及时发现医院信息系统安全管理落实及安全技术实施中存在的不足及风险等。 | 全年 |
| 保障服务 | 针对重大活动、敏感时段，需驻场人员现场预警、日常安全监控与分析；对攻击事件进行分析与应急处置；对防护设备进行调优；调整防御策略；对重要系统服务提供7\*24小时的监测服务与应急响应并提供报告。 | 重大活动、敏感时段 |
| 安全培训 | 对医院全院人员进行安全意识培训，内容包括个人信息保护，日常终端的安全使用，安全事件的引发注意事项等，主要目的提高医院人员的安全意识。 | 1年4次 |
| 安全制度管理与建设 | 协助用户按照等保2.0三级标准建立规范的管理制度、建立定期的培训机制、建立紧急事件应急机制及其各系统等保整改服务。 | 1项 |
| 应急响应服务 | 对网络入侵、拒绝服务攻击、大规模病毒爆发、主机或网络异常事件等紧急安全问题提供应急响应，控制事态发展；保护或恢复客户主机、网络服务的正常工作。 | 全年 |
| 应急演练 | 在服务期内，协助医院信息科开展应急演练，模拟服务器遭黑客攻击等情况的应急处理，全体演练参与人员按照预先制定的演练方案及流程，通过模拟日常工作中遇到的网络攻击、病毒攻击、系统崩溃和网络故障等信息系统突发情况进行基于场景化的演习。 | 1年2次 |
| 运维工具软件 | 需提供符合本项目运维要求的专用运维软件 |
| **网络技术支持服务** |
| 网络调整与优化 | 根据网络环境和需求的变化、新业务上线等，协助用户进行网络调整、升级和改造，以发挥网络最优最完善的服务。 |
| 应急响应服务 | 对医院网络提供应急响应服务，包括远程响应和现场服务 |

**二、服务内容要求**

一）、基础服务

（1）电话支持服务

服务商电话响应热线，电话响应热线7\*24的全天侯不间断的电话服务和信服务。本项目可通过电话响应中心在线支持服务获得直接的技术支持、咨询，以及获取快速技术支持响应。

（2）邮件支持

服务商应具备邮件服务系统，当本项目发生故障需解决问题时，可通过邮件的方式会对问题进行报障。在邮件服务系统接收到故障情况后，工程师将问题录入导系统中，并且会对用户信息及问题进行详细地分析和判断，保障本项目业务稳定运行，需于第二个工作日内回复。

（3）远程支持

服务商对于本项目提供7\*24小时的远程服务，远程服务的方式有电话、QQ、MSN、网站、EMAIL等，并提供解决方案，若不能排除故障，需升级现场支持继续解决故障。

（4）现场支持

当服务商收到本项目报障或服务请求后，服务商根据服务级别和相关要求进行响应，对于无法在电话中解决的问题，及时安排现场人员到用户现场进行故障的处理，以下为现场支持服务响应级别要求：

|  |  |  |
| --- | --- | --- |
| 故障级别 | 响应时间 | 解决方案 |
| I级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失。 | 10分钟内响应，2小时内到达现场 | 12小时以内提供 |
| II级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。 | 30分钟内响应，3小时内到达现场 | 24小时以内提供 |
| III级：属于安全问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。 | 60分钟内响应，4小时内到达现场 | 48小时以内提供 |
| IV级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。 | 4小时内响应，12小时内处理 | 96小时内提供 |

二）、数据库服务要求

1、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。

2、紧急故障处理服务

服务商必须提供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，3小时内到达现场，并必须连续进行维修，直到正常运行。

▲3、数据库专家现场支持服务

服务商需要具有Oracle OCP认证数据库技术人员可在服务期内提供数据库专家现场技术服务，内容包括：数据库安装帮助；数据库升级的规划和实施；数据库的重新规划；故障硬件更换；现场问题的诊断及分析；实施问题的解决方案；设备性能调整等。

4、Oracle数据库备份系统维护

提供Oracle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：

1）系统数据在线数据备份和恢复规划；

2）系统数据在线数据备份和恢复方案的实施；

3）系统数据在线数据备份和恢复方案的测试；

4）系统数据备份和恢复方案的培训；

5、数据库灾难恢复演练

提供Oracle数据库的容灾数据库灾难恢复演练服务，包括：

1）制定容灾数据库灾难恢复演练实施文档；

2）定期协助客户共同实施灾难恢复演练；

3）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。

▲6、数据库可靠性服务（性能调优、性能诊断）。

服务商通过自有的数据库软件工具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：

1）对数据库系统进行自动巡检、监控；

2）查找引起数据库性能下降的各种原因，制订解决方案；

3）根据业务特点及数据库状态，制定数据库调优方案；

4）在业务允许的情况下，对系统做好备份准备；

5）在业务允许的情况下，调整数据库；

6）测试数据库，保证数据库的可用性；

7）协助测试应用软件，检测调优的有效性。

7、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。

8、数据库健康检查和整改服务（巡检服务）

定期到现场进行系统巡检。并提交相应的巡检报告和数据库稳定性评估报告，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。

对数据库巡检中发现的问题，维护公司需在巡检后一周内及时和客户沟通，如果能通过修改数据库配置等技术方式来解决的，维护公司需提供相关的解决方案和步骤，并在客户允许的情况下实施变更。

三）、安全服务要求

**▲**1、服务商为医院提供专业化信息安全服务（一年），负责完善医院现有的信息安全体系，包括制定医院的信息安全目标、完善安全管理制度、设立安全基线、完善日常信息安全作业指导书、编制应急处置流程等，并提供1名信息安全工程师派驻医院现场，按照安全体系的要求开展信息安全日常工作，对于复杂的安全问题，提供二线技术团队支持。

**▲**2、服务商需提供1名专职的信息安全工程师（一年以上运维经验）到医院驻点服务（一年），对已部署的安全产品提供运行维护和技术支持服务，包括日常巡检维护、安全策略优化、故障处理、应急处理等，形成报告，达到安全风险有预防、安全事件有记录、出现问题可追溯的信息安全监控状态，保障医院各系统正常、安全、稳定、高效运行。

**▲**3、现场驻点工程师要求：必须拥有1年以上在相关行业从事网络安全现场驻点运维经验，具有CISP认证资质。

**▲**4、每季度提供1次对医院目标系统的人工渗透测试服务，并出具详细测试报告及修复实施报告。

1. 每月提供不小于1次针对医院关键数据中心的漏洞扫描服务（一年），并出具详细测试报告及修复实施报告。
2. 提供系统上线前安全评估服务（一年），包括物理环境、网络设备、操作系统、应用软件、代码程序和数据等。系统上线前安全评估服务的实施时间应在应用系统完成编码与测试阶段，部署至生产环境后正式发布前。并出具详细测试报告及修复实施报告。
3. 提供安全加固服务，梳理资产并实时更新（一年），包括各种网络设备、安全设备、主机、服务器操作系统、数据库、中间件及安全基线相关等的安全加固及调优测试，含等保安全技术服务，等保整改。
4. 安全建设配合响应，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。

（1）安全漏洞扫描服务

安全风险评估，能准确发现系统的安全隐患，通过评估可以全面了解信息系统的安全现状，而在安全评估过程中，安全扫描服务则是不可缺少并且可以独立存在的一步工作，通过安全扫描工作，可以详细的了解当前网络和系统中可能存在的潜在安全隐患，从而为进一步通过技术手段降低或解决问题提供了参考依据和方法。

安全扫描服务主要使用技术手段，通过现场安全扫描设备方式对被评估对象进行一系列的安全探测，以发现网络中和系统中可能存在的安全隐患。

安全扫描过程中主要是通过评估工具以远程扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。安全扫描项目包括如下内容：

* 信息探测类
* 网络设备与防火墙
* RPC服务
* Web服务
* CGI问题
* 文件服务
* 域名服务
* Mail服务
* Windows远程访问
* 数据库问题
* 后门程序
* 其他服务
* 网络拒绝服务(DOS)
* 其他问题

服务商应定期对客户数据中心机房内的数通设备、服务器、存储、操作系统以及相应中间件进行安全漏洞扫描，提供每月不少于一次的例行安全漏洞扫描，每季度不少于一次的全面性安全漏洞扫描（扫描报告及修复建议根据招标人需求提供）。

（2）安全配置核查服务

目前客户数据中心机房设备种类包含：交换机、防火墙、服务器、存储等硬件设备。服务商需定期派遣专业人员到现场对上述设备进行安全配置核查服务。

配置核查服务，通过自动化的进行安全配置检查，从而节省传统的手动单点安全配置检查的时间，并避免传统人工检查方式所带来的失误风险，同时能够出具详细的检测报告，使客户全面了解当前系统的配置情况，大大提高检查结果的准确性和合规性，节省时间成本，让检查工作变得简单。

配置核查服务主要使用评估工具，通过远程的方式对被评估对象进行一系列的安全探测，以发现网络中和系统中可能存在的不安全配置项与安全隐患，包括操作系统、网络设备、数据库、中间件等设备及系统的安全配置加固建议。配置核查项目包括但不限于如下内容：

* 《◆◆操作系统安全配置规范》
* 《◆◆操作系统安全配置核查规范》
* 《◆◆数据库安全配置规范》
* 《◆◆数据库安全配置核查规范》
* 《◆◆操作系统安全配置规范》
* 《◆◆防火墙设备安全配置规范》
* 《◆◆防火墙设备安全配置核查规范》

（3）对公网站扫描服务

在本次信息安全系统服务中，服务商需要通过对佛山市第四人民医院的对公网站结构分析，目录遍历探测，隐藏文件探测，备份文件探测，CGI漏洞扫描，用户和密码猜解，跨站脚本分析，SQL注射漏洞挖掘，数据库挖掘分析等几个方面进行测试，得出了网站系统存在的安全风险点，针对这些风险点，提供相对应的安全报告，修复并输出报告。

需提供专用WEB应用扫描软件首先对站点进行分析，获取目标应用系统的组织结构，自动找出可能存在问题的程序，对于无法准确判断结果的程序，我们的WEB应用扫描软件提供了交互式漏洞挖掘工具，可以准确判断目标应用系统是否存在安全漏洞，并提供如下漏洞统计表格及安全评级：

漏洞类别进行统计，如下所示:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **漏洞类别** | **高** | **中** | **低** | **风险值** |
| 目录遍历探测 | － | － | － | 0 |
| 隐藏文件探测 | － | － | － | 0 |
| 备份文件探测 | － | － | － | 0 |
| CGI漏洞扫描 | － | － | － | 0 |
| 用户和密码猜解 | － | － | － | 0 |
| 跨站脚本分析 | － | － | － | 0 |
| SQL注射漏洞挖掘（含数据库挖掘分析） | － | － | － | 0 |
| **风险总值** | **0** |

9、提供每季度安全巡检服务，梳理资产并实时更新（一年），包括医院各类信息安全、网络安全、终端安全系统的日常巡检和运维保障。定期巡查安全产品运行状态；根据实际需要进行策略调整，备份；定期对行为审计事件进行分析、评审、处理，发现可疑行为，形成安全事件分析报告。对堡垒机、入侵防护、防病毒系统、威胁发现和应用防火墙等产品，应定期提醒用户特征库的升级并形成记录。

提供定期对客户安全设备的日志进行深入分析和审计，包括对防火墙、IDS、防病毒系统、动态口令认证、日志分析系统等的运行状态、运行事件、日志和关键配置文件进行收集、分析，并提交相应的安全建议。

本地安全巡检服务内容如下：

（1）协助用户制定安全设备巡检计划和巡检规范。

（2）定期对用户的网络安全设备进行巡检。

（3）协助用户分析和解决在巡检中发现的问题。

（4）提交巡检报告。

客户提供以下协助配合服务商的服务：

（1）协助设备检查，必要时提供操作的权限。

（2）确定巡检规范和报告的模版。

10、提供安全加固服务，梳理资产并实时更新（一年），包括各种网络设备、安全设备、主机、服务器操作系统、数据库、中间件的安全加固及调优测试。

针对漏洞扫描、安全评估过程中发现的各种安全隐患、系统漏洞，通过打补丁、修补漏洞、增强安全配置、优化系统架构或调整安全策略等方式及时对系统进行安全加固，范围可覆盖资产梳理、物理检查、管理体系优化、人工检查、漏洞扫描结果加固、渗透测试结果加固(涉及数据库加固)，提高系统的安全性和抗攻击能力，将涉大系统的安全状况维持在较高的水平，减少安全事件发生的可能性。

系统安全加固是指通过一定的技术手段，提高信息系统的操作系统、数据库系统或网络设备安全性和抗攻击能力。常见的安全加固服务手段有：

* 基本安全配置检测和优化
* 提供访问控制策略和工具
* 增强远程维护的安全性
* 系统升级与补丁安装

加固正确实施后，经过良好配置的系统或设备的抗攻击性有极大的增强。在对系统作相应的安全配置后，结合定期的安全评估和维护服务就使得系统保持在一个较高的安全线之上。

**11、以下是安全加固服务要求：**

（1）安全加固的主要范围

针对不同的设备（如交换机、路由器、防火墙等）、不同的操作系统（如NT、UNIX、LINUX、Solaris等）提供安全加固服务，针对不同的应用（如Web服务、FTP服务、E-mail服务、数据库应用等）提供安全加固的建议。包括补丁、停止不必要的服务、升级或更换程序、除去恶意程序、提供修改配置及权限建议、以及针对复杂问题的专门解决方案。根据网络安全评估的检测结果为依据，完全、彻底地堵住这些安全缺陷和漏洞、去除这些薄弱环节。

（2）安全加固的主要策略

**操作系统安全加固和优化**

根据评估报告进行打补丁、升级、修补、加固和优化，提供详细操作报告。

**网络设备安全加固和优化**

网络设备的安全始终是信息网络安全的一个重要方面，攻击者往往通过控制网络中设备来破坏系统和信息，或扩大已有的破坏。网络设备包括主机和网络设施（交换机、路由器等）。

对网络设备进行安全加固的目的就是减少攻击者的攻击机会。

如果设备本身存在安全上的脆弱性，则它们往往会成为攻击者攻击的目标。网络设备的安全脆弱性包括：

* 提供不必要的网络服务，提高了攻击者的攻击机会；
* 存在不安全的配置，带来不必要的安全隐患；
* 不适当的访问控制；
* 存在系统软件上的安全漏洞；
* 物理上没有得到安全存放，容易遭受临近攻击（close-in attack）；

针对这些安全弱点，提出如下几点设备的安全加固技术建议：

* 禁用不必要的网络服务
* 修改不安全的配置
* 利用最小特权（Least-Privilege）原则严格对设备的访问控制
* 及时对系统进行软件升级
* 提供符合IPP要求的物理保护环境

网络安全设备的安全加固和策略配置优化

主要针对防火墙系统、入侵检测系统、数据备份与灾难恢复系统等网络安全设备进行修补和加固，按照安全策略协助厂商进行安全配置和优化。包括：网络安全设备的安全配置，网络安全设备的安全加固，网络安全设备的优化配置等。

网络安全设备的安全始终是信息网络安全的一个重要方面，攻击者往往通过控制网络中的安全设备来破坏系统和信息，或扩大已有的破坏。

所有安全设备或系统，基于网络安全管理的要求，部署相关安全控制策略，实现安全区域的隔离，对办公网、互联网连接数据中心网络进行访问控制，关闭与业务无关的网络端口、协议，实现数据中心安全隔离。

建立终端及外网对内网服务器访问权限的控制，封闭非业务访问端口和非授权终端的访问。对运行授权访问进行精细化访问策略控制。实现应用服务器和数据库服务器之间访问控制，防止服务器之间权限交叉的问题。

通过防火墙对高危的网络端口进行封闭，对于应用需要的端口采用最小化开放原则，减少病毒及威胁的内部传播。

对RDP、SSH、telnet 等运维管理端口进行封闭，只允许堡垒机IP 访问服务器运维端口，实现服务器统一运维管理和审计。

针对医院对外业务访问控制策略，按照业务访问数据流采取单向访问控制策略，基于端口最小化开放原则，仅开放必要的应用端口，应用无关端口一律关闭，确保对外业务区安全。

完成所有安全设备安装实施调试，并与现有设备进行整体联调测试，统一规划优化及配置医院信息安全策略，满足《信息系统安全等级保护基本要求》（GB/T 22239-2008）信息系统安全等级第三级的要求。

12、服务商成立应急技术支持小组，由3人以上技术专家级工程技术人员组成，7\*24小时提供紧急响应服务。当医院网络及信息系统出现服务人员无法解决的信息安全事件时，应立即启动紧急响应服务，协助处理信息安全事件。小组人员应15分钟内响应，2小时内到达现场。响应服务完成后服务单位需整理详细的事故处理报告，内容至少包括事件原因分析、已造成的影响、处理办法、处理结果、预防和改进建议等。

（1）安全事件的定义

安全事件是指网络或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、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。

如发生以下情况，可定义为安全事件：

* 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；
* 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；
* 拒绝服务，正常用户不能正常访问服务器提供的相关服务；
* 系统性能严重下降，有不明的进程运行并占用大量的CPU处理时间；
* 在系统日志中发现非法登录者；
* 发现网络大面积爆发计算机病毒感染；
* 发现有人在不断强行尝试登录系统；
* 系统中出现不明的新用户账号；
* 管理员收到来自其他站点系统管理员的警告信，指出系统可能被威胁；
* 文件的访问权限被修改；
* 因安全漏洞导致的系统问题；
* 其他的入侵行为。

根据事件危害程度，主要分为：

* 安全事故
	+ 由于安全原因造成的网络通信物理或逻辑中断的事故。
	+ 由于安全原因系统重要业务运行停止造成的事故。
	+ 系统重要业务数据损坏。
	+ 系统遭受入侵，机密数据外泄。
	+ 因安全隐患可能会造成事故的现象。
* 严重安全事件：
	+ 由于安全原因造成的网络通信物理或逻辑中断的严重故障。
	+ 由于安全原因系统重要业务运行停止造成严重故障。
	+ 系统部分重要业务数据损坏。
	+ 系统遭受入侵，部分机密资料外泄。
	+ 因安全隐患可能会造成故障的现象。
* 一般安全事件
	+ 由于安全隐患或系统遭受入侵、尝试性入侵但未造成不良后果的网络通信或系统业务运行中出现的一般故障，或利用本网发起的对其他网络的攻击。

（2）安全事件处理时限：

* 事件处理响应时间：
	+ 严重安全事故：10分钟
	+ 安全事件：30分钟
	+ 一般安全事件：60分钟
* 事件处理到场时间：
	+ 安全事故：3小时
	+ 严重安全事件：2小时
	+ 一般安全事件：必要时到场
* 事件初步处理时间（指受影响的通信或者业务恢复网络通信的状态，不包括系统或数据受到损坏需要从备份介质恢复的工作和时间）
	+ 安全事故：3小时
	+ 严重安全事件：6小时
	+ 一般安全事件：一个工作日
* 事件最终处理时间：
	+ 安全事故：24小时
	+ 严重安全事件：24小时
	+ 一般安全事件：三个工作日

（3）安全事件处理报告

安全事件处理完毕后，应尽快提交安全事件处理报告，报告内容应包括事件描述、处理过程、经验及总结等。

13、安全建设配合响应，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。

14、安全培训

安全是动态发展的，黑客攻击手段在不断更新，新的病毒程序也不断产生。安全培训，帮助及时掌握最新的安全技术。提供服务的单位应提供专业安全培训，具体培训内容和时间由双方协商，内容可包含帮助用户了解网络安全基础知识；熟练使用防火墙等安全产品；熟悉解决网络安全故障的常用方法和手段；熟练使用网络安全评估技术；掌握网络安全加固的方法等。

**（1）培训方式：**

安全培训可根据用户要求采用现场培训或集中培训的方式，集中培训将面向管理人员、设备维护人员和安全人员。现场培训主要是客户数据中心机房信息安全的培训，主要针对佛山市第四人民医院的信息系统管理维护人员和安全人员，

* **集中培训**

供应商将组织佛山市第四人民医院的系统管理及维护人员进行关于将要实施的信息安全服务的主题培训，内容包括但不限于信息系统安全基本概念和技术原理、主要安全设备功能介绍及管理配置，同时还要讨论符合如何应对国家针对不断变化的等级保护标准体系的框架。

集中培训场地由佛山市第四人民医院提供。

* **现场培训**

供应商需派遣专业的安全工程师到我院实际机房设备环境中，结合具体的实施经验及方案，详尽地进行设计、安装、配置及维护的安全培训。

▪ 了解信息安全在医院信息化建设中的重要性和必要性

▪ 熟悉网络安全架构的设计要求

▪熟悉各种安全设备的的安全操作规范、条例

▪对一般性故障进行诊断、定位、排除和恢复的方法

▪如何使用各安全厂商的在线服务，查阅各种系统操作和维护手册

**（2）培训对象：**

本项目的培训对象为佛山市第四人民医院信息科的管理、使用、维护人员。人员范围包括各部门工作人员与业务管理人员。

从系统培训对象上来看，主要包括以下人员：

1. 系统操作人员

对系统操作人员的培训，目标是使他们具有更好的计算机专项知识，了解相关应用软件的功能、结构、内容，能熟练地使用操作应用软件。

1. 系统管理维护人员

对系统管理维护人员的培训，目的是使他们具有系统的计算机知识，熟悉计算机系统、网络系统和应用网络系统，能管理和维护系统平台及应用软件，排除一般常见故障，进行日常维护，保证系统正常运行。

以下为部分培训内容要求参考：

|  |  |
| --- | --- |
| 培训内容 | 培训对象 |
| 风险评估 | 专业技术人员 |
| 安全域的确定与划分 | 专业技术人员 |
| 信息安全等级保护 | 普通员工、专业技术人员 |
| 国家对信息系统的安全监管 | 普通员工、专业技术人员 |
| 信息系统安全管理体系 | 专业技术人员 |
| 信息系统安全的层次关系 | 专业技术人员 |
| 信息系统安全运行与维护体系 | 专业技术人员 |
| 防病毒 | 普通员工、专业技术人员 |
| 网络安全及防火墙技术 | 专业技术人员 |
| 操作系统安全 | 普通员工、专业技术人员 |
| 等级保护中的安全功能技术与安全保障技术要求 | 专业技术人员 |
| 入侵防御技术 | 专业技术人员 |
| 漏洞扫描技术 | 专业技术人员 |
| 网络安全管理技术 | 专业技术人员 |
| 应急响应 | 普通员工、专业技术人员 |
| 信息安全工程过程介绍 | 专业技术人员 |
| 实验课程 | 普通员工、专业技术人员 |
| 定制培训内容 | 普通员工、专业技术人员 |

**三、维护工作支持**

**1、服务商提供IT运维工具软件，该软件工具要满足以下要求：**

IT运维工具功能模块包括：移动APP（扫码评价）、用户自助服务、微信报障、合同管理、服务台、事件管理、问题管理、变更管理、配置管理、知识管理、服务级别管理、报表管理（能自动生成各类运维统计报表）者：需提供系统界面图和主要管理流程图,并提供运维工具软件各项功能的演示。

|  |
| --- |
| **功能模块指标要求** |
| **▲**移动APP（扫码评价） （提供系统界面图和主要管理流程图） |
| 用户自助服务（提供系统界面图和主要管理流程图） |
| 微信报障（提供系统界面图和主要管理流程图） |
| 合同管理（提供系统界面图和主要管理流程图） |
| 服务台（提供系统界面图和主要管理流程图） |
| **▲**事件管理（提供系统界面图和主要管理流程图） |
| **▲**问题管理（提供系统界面图和主要管理流程图） |
| 变更管理（提供系统界面图和主要管理流程图） |
| **▲**配置管理（提供系统界面图和主要管理流程图） |
| 知识管理（提供系统界面图和主要管理流程图） |
| **▲**服务级别管理（提供系统界面图和主要管理流程图） |
| 报表管理：能自动生成各类运维统计报表（提供系统界面图和主要管理流程图） |

**四、网络技术支持服务**

1. 网络故障排查

对网络环境中出现的故障进行分析排查处理，保证网络环境正常运行。

1. 网络架构调整与优化

根据医院环境和网络需求的变化、新业务上线等所需网络环境进行调整与优化，协助用户进行网络升级和改造，以发挥网络最优最完善的服务。

1. 应急响应服务

对医院网络提供应急响应服务，包括远程响应和紧急现场服务。

**五、保密要求**

1、本项目服务期及维护过程中的资料，服务商应将保密资料作为商业秘密予以保护，且不得将该保密资料任何部分或全部进行复制或向第三方披露。服务商仅可为本项目确有知悉必要的实施主要人员披露客户提供的保密资料，但同时须指示其实施主要人员遵守所规定的保密及不披露义务。

2、服务商应对根据双方约定接受的保密资料妥善保管。对于保密资料在服务商期间发生的被盗、遗失、不慎泄露以及其他对其保密性存在现实或潜在损害的事件，服务商应承担全部责任，并赔偿客户因此遭受的经济损失（包括但不限于直接经济损失，且以实际遭受损失为限）。本项目服务期及维护期结束或保密协定解除后，一方必须销毁所有保密资料的复制件并将原件返还给另一方。

3、法律或有管辖权的法院要求服务商披露的，服务商应在合理的时间提前通知客户，使其得以采取其认为必要的保护措施。

**六、服务期：自合同签订生效之日起提供一年的数据库系统与安全运维服务。**

**七、付款方式：**

1、签订合同后，服务商给客户开具合同总额10%、有效期至 年 月 日的银行保函。

2、每个季度服务商向客户提供季度服务报告、服务详情内容、有效发票等资料，客户在收到资料后于15个工作日内支付服务款，每个季度支付合同金额的25%，即人民币￥ 元，大写： 元整。

3、收款方、出具发票方、合同乙方均必须与服务商名称一致，且须开具含税发票给客户。

4、服务商凭以下文件申请合同款：

（1）合同复印件；

（2）季度服务报告复印件；

（3）服务商开具有效的发票。

**八、售后服务要求及服务质量考核**

1、本服务项目将每季度对服务商的服务成果进行考核，考核项目如下（基础分为100分）

|  |  |  |  |
| --- | --- | --- | --- |
| 考核项 | 考核内容 |  | 扣分分值 |
| 安全事件(服务商因素引起的) | 重大故障，系统瘫痪，无法运行，院级业务停顿 | 4小时及以上 | 5分/次 |
| 2-4小时 | 3分/次 |
| 1小时以内 | 1.5分/次 |
| 受市级及以上管理部门信息及网络系统安全事件通报或下发整改通知书 | 3分/次 |
| 影响和限制了部分业务运营 | 4小时及以上 | 3分/次 |
| 2-4小时 | 2分/次 |
| 1小时以内 | 1分/次 |
| 重大故障2小时未到现场 | 2分/次 |
| 服务质量(服务商因素引起的) | 未按时完成安全服务计划内项目 | 2分/次 |
| 未按时提交文档方案及报告 | 1分/次 |
| 按月检查未能达到安全预警平台指示80分 | 1分/次 |

2、基于医院信息安全的维保是一个长期战略性目标，为保证项目稳定，对服务商、驻场人员每季度进行评分考核及满意度考核。季度考核评分报告表需附到季度服务报告。驻场人员及团队未能通过考核制度设定的指标及满意度考核低于设定分值，客户有权要求更换人员。