**防统方系统项目**

**用户需求书**

### 1.1项目描述

### 为进一步规范我院医疗卫生服务行为，加强行业作风建设，严禁为不正当商业目的统方，维护正常工作秩序。非正常统方行为作为药耗回扣利益链条中的重要环节，触犯了中华人民共和国刑法第285条第2款，将构成非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪。破坏了医疗机构良好的公众形象，降低了医疗机构的社会满意度,这种行为严重影响医疗机构的社会形象，因此我院需要部署控制统方的系统，并保证审查数据保存24个月以上。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **数量** | **防护区域** | **备注** |
| 1 | 防统方系统 | 1套 | 数据中心 | 含硬件 |

### 1.2产品说明

|  |  |  |
| --- | --- | --- |
| **序号** | **功能模块** | **技术规格** |
| 1 | **系统架构** | 1.吞吐量：≥20Gbps  2.SQL事务数/秒：≥300,000  3.接口：支持10/100/1000M自适应电口 \*6(可扩展SPF多模光纤，最多扩展至4个)  ★4.内存：≥64GB，处理器：两颗CPU，每颗CPU八核心十六线程，主频：≥3.3GHz，动态加速频率≥4.7GHz，LM3缓存≥16MB，TDP功耗 ≤95W 存储：≥24TB，使用RAID保护，日志不少于24个月，电源：N+1冗余电源  5.对数据中心进行全面的防统方监控与审计 |
| 6.管理、使用用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。 |
| 7.系统支持双密码用户。 |
| 8.所有系统数据都支持加密传输，防止信息外泄。 |
| 9.系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。 |
| 10.具备用户行为记录功能，记录用户所有的操作（业务访问、系统维护、策略配置等）。 |
| 11.系统配置文件支持导入、导出。 |
| 12.采用B/S架构，提供中文WEB管理界面以便于管理。 |
| 13.支持集群,系统支持冗余备份。 |
| 14.支持双向对接医德医风系统进行展示。 |
| 15.系统内置故障排错系统，判断故障所在，帮助管理人员快速排查问题。 |
| 2 | **防统方模块** | 16.内置防统方知识库，且具有独立自主统方学习功能，帮助医院深化党风廉政建设和反腐败工作,规范药品统计权限管理。支持对接医院智慧党建平台进行管理，具有该智慧党建对接模块的《软件著作权登记证书》。 |
| 17.系统应用大数据人工智能建模分析检索非法统计医嘱\处方，并生成报告和相关建议规则反馈给医院，该大数据分析功能具有版权。 |
| ▲18.旁路部署，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统能独立完成审计数据采集和防统方告警，不依赖于数据库自身审计日志系统，不得在现有服务器上安装可能带来风险的程序。 |
| 19.分析可疑对象的信息，包括IP、端口、MAC、主机名、程序信息、数据库连接信息。 |
| 20.从业务流程角度入手，结合核心数据特征，提供了高度集成的“事前+事中+事后”数据防护手段，获得《信息化创新医疗服务模式》认证。 |
| 21.应用云计算功能提供数据分析平台，对用户提交的数据进行自主分析，并生成报告和相关建议规则反馈给用户。 |
| 22.支持医院信息管理系统多层结构，提供全方位的三层（应用层、中间层、数据库层）的访问审计，三层关联必需支持自动关联，以提升关联准确度和审计人员追踪索源难度，同时需要支持手动关联，可以直接追踪到前端业务的操作人员IP地址、MAC地址和用户。 |
| ▲23.抗菌药物中不少为贵重药品，可能存在药品使用回扣等腐败现象，需预留一定的接口，支持双向对接抗菌药物用量管理系统进行展示，具有抗菌药物用量管理系统《软件著作权登记证书》，支持对指定时间内全院抗菌药物品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的抗菌药物品种进行分析，以便医院了解可能存在回扣的药品，提供产品截图。 |
| ▲24.支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的操作审计监控，该医院内部审计管理模块具有《软件著作权登记证书》。 |
| 25.能够出具针对纪委、监察室相关人员使用的审计报告（支持每天或多天生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持对接清廉医院管理系统，具有该模块的《软件著作权登记证书》。 |
| 26.可疑对象定位功能，可以精确定位可疑对象的物理位置。 |
| 27.统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP地址、客户端工具、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。 |
| 28.支持对双向数据包的解析、识别及还原，不仅对请求进行实时监控，而且还可对返回结果进行完整的还原，根据非法统计医嘱\处方行为的特征实时告警，提供产品截图。 |
| 3 | **数据库审计管理** | 29.从审计主体、审计客体、日志格式、规则分析能力、报表、告警、存储等模块完全按照等级保护基本要求和测评要求设计研制，该“防统方”系统模块取得《中国国家信息安全产品认证证书》。 |
| 30.支持对Oracle、MS-SQL 、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase 等数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于6个，并且可以是一个oracle库而另外一个是其他。 |
| 31.主动/被动方式监控关键服务器的开放端口，提供扫描现有应用系统的漏洞。 |
| 32.用户可以根据需要自定义规则，并能根据设定的条件产生审计报告。能对审计结果进行多条件组合查询，比如按下列条件查询：IP地址、MAC地址、表名、操作方式、计算机名、数据库名、程序名等。并就能支持按关键词进行模糊查询。查询结果应支持多种格式(excel、pdf、txt等)导出。 |
| 33.系统可以监控、记录并且还原客户端连接到服务器的TELNET/FTP等远程登录操作信息，记录内容包括客户端IP地址，客户端MAC地址，服务器地址以及产生记录的时间，并提供多种查询，支持多种文件格式导出。 |
| 34.支持指定非关注策略，系统将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。策略因子包括：数据库操作来源IP地址、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句（DDL、DML、DCL）、数据库表组（表、列）等。 |
| 35.提供数据库登录用户名称异常探测、数据库操作源终端异常探测、数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测，可设定异常黑白名单，对客户端地址、客户端程序、数据库账号、客户端用户名以及执行结果等异常的行为进行异常告警，支持自主学习能力。 |
| 36.系统能支持多个网段客户端对数据库操作行为的会话审计，能够对各种访问数据的途径（如客户端软件、PL/SQL、SQL\*Plus、PB、Toad等各种SQL操作工具）进行监控和设计，可以跟踪审计某某时间、某某IP、某某计算机名、某某用户对数据库服务器进行了该类操作。 |
| 37.能够检测网络拷贝等操作,能够检测通过网络KVM发出的指令。 |
| 38.系统能支持对数据库SQL操作语句的详细审计，可以分析出每条语句的操作方式、表名、存储过程名、详细操作内容，执行时长、操作成功/失败，受影响行数，关联表与关联表数等字段信息，可审计并还原SQL操作语句。 |
| 39.可根据SQL执行的时间长短设定规则，如命令执行时长超过30秒进行告警；可根据返回记录数多少设定规则，如SQL操作返回的记录数或受影响的行数大于等于10000行时进行告警。 |
| 4 | **告警模块** | 40.可根据用户自定义规则实时发出手机短信通知\App和邮件提醒等多种方式的告警信息，该移动端管理功能具有版权，并支持配备相应的告警信息发送设备。 |
| 5 | **服务要求** | ★41.系统免费升级与维护期为六年，实施上线、维护工作必须由原厂厂家完成；必须在合同签订后30个工作日内完成系统调试、上线和初验，初验后开始试运行并在试运行3个月后进行最终验收。提供7\*24小时电话、现场的维护、软件升级服务；每季度至少提供一次巡检及协助报告分析服务。当收到医院的报修要求时，若2小时内电话无法解决，4小时内到达现场进行维护，48小时内解决完毕。 |