合同编号：

陕西省交通医院廉洁风险防控系统

维保合同

甲方：陕西省交通医院

乙方：陕西证联信息技术有限公司

甲方：陕西省交通医院

住所地：西安市大学南路 276 号

法定代表人：杜建革

乙方：陕西证联信息技术有限公司

住所地：西安市雁塔区高新一路 40 号万科金域国际 B 座 1512 室

法定代表人：杨鸿胤

为了保证甲方医院公立医院廉洁风险防系统稳定、可靠的运行，并能及时解决系统运行中可能出现的故障，甲乙双方依据国家有关法律规定，经过平等协商，就甲方医院公立医院廉洁风险防系统维护达成如下协议。

第一条　售后服务内容及人员要求

1. 本项目专属技术团队人员不少于 5 名，团队人员须满足以下资质要求：

- 项目负责人须具备 3 年以上医疗信息化系统运维项目管理经验；
- 技术团队须包含至少 1 名数据库工程师、1 名网络安全工程师，所有运维人员须具备对应系统的原厂运维认证资质；

乙方负责甲方在用的、由乙方提供的公立医院廉洁风险防系统（详见附件：公立医院廉洁风险防系统维护范围清单）的维护工作，具体服务方式及内容如下：

序号	服务项目	服务内涵	服务方式	服务频次 / 次数要求
1	信息系统基础运维服务	1. 附件 1 所列全部系统模块的软件操作指导、故障排查、bug 修复、配置管理服务； 2. 系统死机、数据错误、监管预警失效、防统方监测异常等全场景故障处置； 3. 系统运行环境适配、显示异常、运行效率降低等问题的优化处置； 4. 系统与院内其他信息系统的接口运维、适配调整、故障修复； 5. 系统终端设备、服务器运行状态的定期巡检与隐患排查。	7×24 小时热线服务、安全远程运维服务、现场驻场 / 上门服务	不限次数，全时段响应

2	数据库专项运维服务	1. 每月开展数据库全量巡检，检查内容包括服务器系统日志、磁盘空间、CPU / 内存使用率、数据库表空间、数据文件大小、数据库运行日志、异常操作审计日志等； 2. 每季度完成数据库安全加固、高危漏洞修复，确保数据库符合等保合规要求； 3. 提供同版本数据库迁移、数据备份与恢复服务； 4. 针对巡检发现的问题，完成数据库性能优化、参数调整； 5. 数据库故障的应急处置，保障廉政监管数据、审计数据不丢失、不泄露、不篡改。	热线服务、安全远程服务、现场服务	不限次数，每月至少 1 次全量巡检，每季度至少 1 次性能优化，每年至少 2 次备份恢复演练
3	信息系统升级更新服务	1. 依据国家、省、市卫健、纪检、网信等部门政策变更，免费、及时完成系统合规性适配与更新； 2. 提供系统同版本内免费升级、功能优化服务； 3. 定期完成系统安全补丁、漏洞修复包安装调试，每月完成高危漏洞排查修复。	现场服务为主、远程辅助	不限次数，每月至少 1 次安全补丁更新，政策变更后 10 个工作日内完成合规适配
4	防统方系统专项更新服务	1. 严格依据陕西省卫健委相关文件要求完成系统升级； 2. 实现审计报告自动生成、自然语言翻译、权限分离、自我学习、加密传输、双密码、操作审计、故障排查、配置导入导出、应用层追踪、旁路部署、对象定位、白名单、自定义规则、核心数据监控、多层审计、B/S 架构、数据包解析、远程操作记录、可疑数据	现场服务	不限次数

		回放、接口预留等全部要求功能。		
5	网络安全与数据安全服务	1. 严格按照《网络安全法》、《数据安全法》、《个人信息保护法》提供网络与数据安全服务； 2. 网络安全：漏洞修复、安全整改、风险排查、入侵防御； 3. 数据安全：数据加密、备份恢复、数据库审计、廉政数据全生命周期保护； 4. 配合完成等保测评、数据安全检查、廉政监管专项检查。	远程服务、现场服务	不限次数，每月至少 1 次安全风险排查
6	人员培训服务	1. 针对管理岗、操作岗、信息科制定差异化培训计划与教材； 2. 培训内容：系统操作、故障处置、廉政监管要求、数据安全、应急流程； 3. 培训后组织考核； 4. 系统升级、政策调整后提供专项培训。	现场培训、远程线上培训	全年累计不少于 20 学时，集中培训不少于 2 次，专项培训不限
7	应急保障服务	1. 针对系统瘫痪、数据泄露、网络攻击、防统方失效等制定专项应急预案； 2. 每年联合开展不少于 2 次应急演练； 3. 重要检查、节假日等特殊时段提供驻场保障。	现场驻场服务、7×24 小时应急响应	每年不少于 2 次应急演练，特殊时段按需驻场
8	服务器端国产化替代专项技术服务	1. 国产化适配前置评估：针对采购人服务器端国产化替代建设需求，完成现有《公立医院廉洁风险防控系统》、《防统方审计系统》全模块、全功能的国产化环境兼容性评估，覆盖国产服务器硬件、操作系统、数据库、中间件的全栈适配性分析，出具完整评	现场服务为主，远程辅助服务，专项驻场服务	按需提供全流程服务，服务期内不限响应次数；迁移

		估与实施方案； 2. 原厂级适配改造开发：针对评估发现的兼容性问题，提供系统源代码级的适配改造、功能优化、接口重构服务，确保系统在国产化服务器环境下全功能正常运行、业务流程无断点、数据交互无异常，同时保障系统与院内 HIS、LIS、PACS、EMR 等现有及新增信创/非信创系统的互联互通，适配改造后系统性能不低于原有非国产化环境水平； 3. 国产化迁移与割接实施：配合采购人完成国产化测试环境搭建、全量功能测试、压力测试、兼容性测试、安全测试，制定分阶段、零风险的业务割接方案，割接操作安排在非业务高峰时段（夜间、节假日），全程派驻技术人员现场值守，保障迁移过程医疗数据零丢失、零泄露、零篡改，业务中断时长符合医院医疗安全管理要求，如出现异常立即启动回滚预案，保障业务连续性； 4. 国产化环境专项运维保障：系统迁移至国产化服务器环境后，提供专属专项运维服务，包括国产化环境下系统日常巡检、性能优化、故障排查处置、安全补丁适配、漏洞修复、合规性升级，建立国产化环境专属运维台账，针对国产化平台特性优化运维流程，保障系统在国产化服务器环境下持续稳定运行； 5. 合规适配与测评支撑：配合采购人完成信创建设合规验收、网络安全等级保护测评、医院信息互联互通标准化成熟度测评等		完成后每月至少 1 次国产化环境专项巡检，每季度至少 1 次性能优化

		相关工作，提供系统国产化适配证明、测试报告、技术支撑及整改服务，确保系统符合国家及地方交通、卫健、网信部门关于医疗信息化信创建设的最新政策要求； 6. 国产化专项培训：针对国产化服务器环境下的系统运维、操作使用、故障应急处置，为采购人信息科技术人员、医护操作岗、管理岗人员提供专项定制化培训，编制专属培训教材，确保参训人员掌握对应技能。		
9	运维报告服务	1. 每季度、每年提交阶段性运维报告，年度报告须包含全年服务总结、系统运行评估、安全合规情况、下一年度运维优化方案等； 2. 重大故障、专项工作单独提交专项报告。	书面盖章报告电子文档	每季度1次季报，每年1次年报，专项报告按需提交

第二条　甲方责任及义务

1. 甲方应按本合同约定及时向乙方支付维护费。

2. 甲方应发现故障后及时向乙方发出维护服务要求。

3. 甲方应向乙方提供相关软件系统正常使用和维护的环境。

4. 甲方所提维护服务需求内容应符合医院实际业务需求，符合国家相关规定。

5. 甲方应安排专人配合乙方运维工程师的维护工作，协助乙方进行需求调研及分析，向乙方提供维护服务所需的必要支持，并对乙方的维护服务过程、结果进行监督、检查、确认、评价。

第三条　乙方责任及义务

1. 专人负责：乙方应指派经验丰富的运维工程师来承担甲方医院信息管理系统的具体维护工作，乙方服务人员应保证相对固定，如需更换人员需提前征得甲方同意。

指定项目负责人：乙方指定【肖博文】为负责人，全权负责日常服务合作事宜，乙方指定联系人发生变化时，应提前【10】个工作日内书面通知甲方。

2. 运维响应：乙方应为甲方提供全年 7*24 小时的电话技术支持、远程网络协助及现场服务；电话服务专线：【 029-88607608】。乙方在合同服务期内按附件 2：《医院信息系统故障分级标准及响应时间明细表》为甲方信息系统提供维护或故障维修，直至系统恢复正常运营。

3. 维护记录：在本合同约定的维护期限内，乙方应建立完善的维护记录管理体系，对于任何维护任务，乙方服务人员应严格填写维护记录单并交由甲方相关负责人审批，每次服务还应由甲方进行评价；服务产生的相关文件应及时归档且双方同时备案。

4. 巡检：乙方应每季度至少【4】次到达甲方现场对相关软件系统进行检查，优化软件系统运行，同时做好相关软件系统运行使用情况的记录；对可能存在的隐患及出现的故障提出解决方案，在征得甲方同意后现场进行软件系统优化；另外，乙方应根据实际需要，现场对甲方信息中心工作人员进行维护方案的培训及实际操作的指导。

5. 数据安全及保密：乙方在软件系统维护过程中，应协助甲方提前做好相关数据的备份工作，保证数据安全，并且做好相关数据及资料的保密工作；未经甲方允许，乙方不得将相关数据及资料带走、传播或它用。

第四条　不可抗力条款

1. 乙方对甲方在使用相关软件系统的过程中，因设备故障、病毒等造成的系统故障、数据丢失，以及因相关软件系统误用、毁损、遗失、被盗或其他不可抗力造成的损失双方均不承担责任，乙方积极协助甲方处理此类问题。

2. 由于特殊情况（非乙方原因所致）及不可抗力造成维护服务拖延或不能正常进行，甲乙双方应按实际情况重新调整维护服务时间和内容，双方同意后执行。

第五条　数据安全与信息保密要求

本条款依据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《医疗卫生机构网络安全管理办法》《医疗卫生数据安全指南》等法律法规及行业规范制定，为本项目刚性要求。乙方须严格遵照执行，独立承担全部合规责任及违约产生的一切法律后果。

1. 制度建设与人员合规要求

乙方须建立健全医疗数据全生命周期安全保护体系、数据安全及个人信息保护管理制度，严格符合医疗数据分类分级、商用密码管理等国家规范。乙方须设立本项目专属数据安全责任部门、配备专职技术运维人员，做到责任到人，并向甲方提交专职人员资质、在岗证明等材料备案，未经备案不得开展项目工作。

2.保密信息界定与使用限制

2.1. 保密信息范围：甲方保密信息包括但不限于本协议内容及履行情况、甲方医疗业务数据、患者个人信息、电子认证数据、涉密信息、经营信息、知识产权、业务规划、财务、人事、技术资料、系统源码、实施方案、业务流程及甲方及其关联机构全部未公开内部信息。

2.2 信息使用规则：乙方在服务过程中接触、获取的甲方全部数据与保密信息，仅限本项目运维服务使用。乙方不得擅自复制、存储、泄露、转让、篡改、销毁相关数据，不得用于商业推广、二次开发、对外共享、自用研究等一切未经甲方书面授权的用途，不得向任何第三方披露、传播或提供甲方保密信息。

3.保密工作机制

乙方须与甲方签订专项数据安全与保密协议，并组织所有项目参与人员逐一签订个人保密协议。保密义务覆盖人员在职及离职后终身有效，协议须明确保密范围、义务边界及违约责任，全部协议文本须提交甲方审核备案。

4.远程运维安全管控要求

乙方开展甲方系统远程运维操作，须事先取得甲方书面审批，全程采用加密安全接入方式，严禁未经授权私自远程操作。所有运维操作全程留痕，审计日志留存期限不少于六个月，严禁依托公共互联网对甲方业务系统开展运维操作。

5.安全事件应急处置与责任承担

乙方须建立数据安全风险防控及应急处置机制。发生数据泄露、篡改、丢失、非法访问等安全事件的，乙方须十分钟内响应，第一时间向甲方书面报备并启动应急预案，采取有效措施控制风险、阻断隐患。乙方须全面配合甲方开展事件调查、溯源、监管上报及整改复盘工作。因乙方管理、操作、制度缺陷导致的安全事件，由乙方承担全部行政、民事、刑事责任，全额赔偿甲方经济损失、商誉损失及维权成本。

6.服务期满数据处理

本协议期满、解除或终止后，乙方须完整、无损移交全部项目资料、运维数据、技术文档及台账材料。移交完成后，乙方须彻底删除其持有的甲方全部数据、备份及留存材料，不得保留任何副本、缓存及备份文件，并向甲方出具数据删除承诺书，接受甲方核验。

7.其他约定

7.1 乙方须无条件配合甲方开展数据安全检查、网络安全审计、等级保护测评、商用密码安全性评估及各类合规核查工作，及时提供相关台账与技术资料，落实问题整改，并自行承担全部整改成本及合规责任。

7.2 除法定强制披露情形外，未经甲方书面许可，乙方不得向任何第三方披露甲方保密

信息。乙方向律所、审计、咨询等合作机构披露的，须前置明确保密义务，并对信息泄露风险承担全部连带责任。

8.违约责任

8.1. 乙方违反本条款任一约定即构成根本违约，须全额赔偿甲方全部直接及间接损失，包括但不限于经济损失、行政处罚费用、律师费、诉讼费、商誉损失等，并承担相应行政、民事、刑事责任。

8.2. 本数据安全及保密条款独立有效，不因本协议无效、解除、终止而失效，乙方对甲方保密信息承担终身保密及安全保障义务。

第六条 服务期限及地点

1.服务期:本项目服务期限为1年，自合同签订之日起计算。服务期内，服务商服务质量持续不达标，采购人有权提前终止合同。

2.合同部履行地点：陕西省交通医院指定地点

第七条 服务费及付款方式

服务费总计：（大写）：贰万玖仟元整 （小写：29000.00元），合同签订生效后，共计分为以下两次进行付款：

付款方式：

1、第一笔款项：双方签订合同后，成交乙方须向甲方开具合法、等额、有效的发票，甲方收到发票后5日内付合同价款的50%；

2、第二笔款项：服务期满后，甲方组织完成年度考核【严格按照本文件附件3《信息系统售后运维服务质量评价标准》执行，评分满分100分。90分（含）-100分为优秀，70分（含）-89分为合格，70分以下为不合格】验收后，乙方向甲方开具剩余合法、等额、有效的发票，甲方收到发票后5日内根据考核结果支付剩余合同价款:

●年度考核结果为优秀的，支付合同剩余50%价款；

●年度考核结果为合格的，扣除合同总价款的10%作为违约金，支付合同剩余40%价款；

●年度考核结果为不合格的，甲方有权不予支付合同剩余50%价款，同时保留追究乙方违约责任的权利。

3.若乙方在甲方付款前未能提供全额合规发票的,甲方有权拒付合同款项,且不承担任何责任,乙方亦不得以此为由拒绝履行任意合同义务。

第八条 知识产权条款

1.本项目涉及系统的软件著作权、知识产权归原权利人所有，供应商仅可基于本项目运

维服务目的，在采购人授权范围内使用相关软件及技术资料，不得擅自复制、分发、转让、反编译、反向工程，不得用于任何其他用途。

2.服务期内，采购人基于系统使用产生的全部医疗数据、业务数据、患者个人信息等所有数据的所有权、使用权均归采购人所有，供应商不得主张任何权利，不得擅自使用。

3.供应商为采购人提供的定制化功能开发、政策适配升级、技术方案等成果，知识产权归采购人所有，供应商仅可保留非商业用途的技术使用权。

第九条 违约责任

1. 本合同违约责任严格按照《中华人民共和国民法典》相关条款执行。

2. 乙方未按合同约定提供服务，或服务质量、响应时效、技术能力不满足合同要求，甲方有权按《服务质量评价标准》扣除对应款项，并要求乙方限期整改；整改后仍无法满足合同要求的，甲方有权扣除对应合同款项，直至单方面解除合同，乙方须承担甲方因此遭受的全部损失。

3. 乙方未按故障 SLA 要求完成响应与故障处置的，每出现一次一级故障超时，扣除合同总价款的 5%；每出现一次二级故障超时，扣除合同总价款的 2%；三级、四级故障超时，按评价标准扣除对应分值，并累计扣除合同款项。因乙方故障处置不及时导致医院业务中断、产生医疗纠纷或监管处罚的，全部责任与经济损失由乙方承担。

4. 乙方违反数据安全与保密约定，发生数据泄露、篡改、丢失等事件，或擅自使用、转让甲方数据的，甲方有权立即解除合同，不予支付剩余全部合同款项，乙方须支付合同总价款 30% 的违约金，同时承担全部法律责任，赔偿甲方因此遭受的全部经济损失（含监管处罚、民事赔偿、商誉损失等）。

5. 乙方未经甲方同意，擅自更换项目核心人员、转包 / 分包本项目服务的，甲方有权扣除合同总价款的 10% 作为违约金，情节严重的，有权解除合同。

第十条 争议解决

甲乙双方在发生合同纠纷时，应本着互谅互让的原则友好协商解决。若协商不成，双方均可向甲方所在地有管辖权的人民法院提起诉讼。

第十一条 通知及送达

1.甲乙双方因履行本协议而相互发出或者提供的所有通知、文件、资料，均应以本协议所列明的联系方式送达，当面交付文件的，在交付之时视为送达；以邮寄方式的，以实际收到日为送达，实际送达日超出 7 日或无法查询投递结果的，均将视为在将通知交寄之后的 7 日按期

送达；以电子邮件发送的，邮件发出并到达对方服务器之时视为送达。有关本协议的通知，任何一方向双方在本协议所填写的地址、手机号码、电话号码、电子邮件、微信号等发送的通知，即视为送达。

2. 双方一致认可，在本协议签订后，双方之间的书面通知等文件通过递送、挂号、传真、特快专递等方式发送至协议记载的双方的通讯地址视为送达，且该通讯地址适用争议解决阶段；如果一方故意拒收、找他人代收、邮件被退回或以其他理由逃避接收文件的，所有书面文书自发出之日视为送达。

3. 任何一方的联络方法发生变更的，应在变更之日起 3 个工作日内书面通知对方。在被通知方收到有关通知之前，被通知方根据变更前的联络方法所做出的联络和通讯应视为有效，未及时通知变更情况的一方自行承担由此产生的法律后果。

第十二条　附则

1. 未经双方书面确认，任何一方不得变更或修改本合同。

2. 对于本合同未尽事宜，双方可随时签订补充协议或以附件的形式对本合同中的有关问题作出补充、说明、解释。本合同的补充协议和附件为其不可分的部分，与本合同具有同等法律效力。

3. 本合同须加盖“骑缝章”，以确保合同的完整。

4. 服务期限满，甲方若需乙方继续提供日常运行维护服务，甲方需与乙方续签技术服务合同，并支付年服务费。

4. 本合同共 18 页一式四份，双方各执二份，甲、乙双方法定代表人或授权代表签字并加盖公章后，方可生效，均具有同等法律效力。

（以下无正文）

甲　　方：	陕西省交通医院（章）	乙　　方：	陕西证联信息技术有限公司（章）
单位税号：	12610000435201944P	单位税号：	91610131MA7FDQ6387
单位地址：	西安市大学南路 276 号	单位地址：	陕西省西安市高新区高新一路 40 号万科金域国际 B 座 1512 室
电　　话：	029-88490077	电　　话：	029-88607608
银　　行：	中国农业银行西安昆明路支行	开户银行：	中国民生银行股份有限公司西安高新科技支行
账　　号：	2614 2601 0400 17869	账　　号：	634 384 023
法定代表人或委托代理人：	章社印建	法定代表人或委托代理人：	
签订日期：	2026 年 11 月 16 日	签订日期：	2026 年 11 月 16 日

附件 1：医院公立医院廉洁风险防控系统维护范围清单：

信息系统名称	子系统名称
公立医院廉洁风险防控系统	职务权力管理
	职业权力管理
	患者满意度评价管理
	供应商诚信度管理
	系统维护功能
	防控专网
防统方审计系统	统方行为实时监测
	审计报告生成
	权限白名单管理
	风险预警与追溯

附件 2：医院信息系统故障分级标准及响应时间明细表

序号	故障等级	故障情况描述	刚性 SLA 要求
1	一级故障（重大）	1. 系统核心服务瘫痪，导致业务中断，多部门终端无法办理业务，严重影响医院正常医疗秩序； 2. 系统与 HIS、EMR、PACS 等核心系统接口完全中断，导致业务数据无法传输，严重影响医院正常医疗秩序 3. 发生患者个人信息批量泄露、医疗数据被篡改/丢失等重大数据安全事件； 4. 系统被非法入侵、攻击，出现高危安全漏洞，威胁医院整体网络安全。	1. 10 分钟内必须响应，与采购人明确故障情况，出具应急处置方案； 2. 4 小时内派驻具备资质的技术人员到达现场； 3. 6 小时内完成故障修复，恢复系统核心业务正常运行； 4. 无法在时限内完全修复的，须提供临时应急方案保障业务连续性，直至系统完全恢复； 5. 故障处置完成后 24 小时内提交正式故障分析与复盘报告。
2	二级故障（严重）	1. 系统操作性能严重降级，核心功能响应延迟超 500%，严重影响医生操作与患者业务办理； 2. 核心科室、门诊 3 个及以上科室系统无法正常使用，影响大面积患者就医； 3. 系统出现数据异常、统计错误，影响医疗业务正常开展，存在数据安全隐患。	1. 30 分钟内必须响应，出具初步处置方案； 2. 6 小时内到达现场或通过安全远程方式完成故障处置； 3. 12 小时内完成故障修复，系统恢复正常运行； 4. 故障处置完成后 3 个工作日内提交故障分析报告。

3	三级故障（一般）	1. 系统非核心功能受损，仅影响单个科室/少量终端使用，医院核心业务可正常开展； 2. 系统出现局部数据异常、报表统计偏差，不影响核心业务办理； 3.配套设备故障，不影响整体业务流程。	1. 30 分钟内必须响应，出具处置方案； 2. 12 小时内到达现场或通过远程方式完成故障处置； 3. 24 小时内完成故障修复，闭环处置问题。
4	四级故障（轻微）	1. 系统出现一般性操作问题、界面显示异常，对患者就医、系统运行几乎无影响； 2. 医护人员提出的系统操作咨询、功能配置调整等非故障类服务请求。	1. 30 分钟内必须响应，提供技术指导与解决方案； 2. 24 小时内通过远程或现场方式完成处置； 3. 48 小时内完成问题闭环。

附件 3：信息系统售后运维服务质量评价标准

本标准为项目考核验收的唯一依据，满分 100 分，具体评分规则如下：

序号	一级评价项目	二级评价项目	分项分值	明细分值	评分标准
1	日常售后运维服务（25 分）	故障响应及时性	10	3	服务期内一级故障响应时间超时（＞10 分钟），扣 3 分/次
				2	服务期内二级故障响应时间超时（＞30 分钟），扣 1 分/次
				2	服务期内三级故障响应时间超时（＞30 分钟），扣 0.5 分/次
				3	服务期内四级故障响应时间超时（＞30 分钟），扣 0.3 分/次
		故障处置与解决时效性	15	5	服务期内一级故障解决时间超时（＞6 小时），扣 5 分/次
				4	服务期内二级故障解决时间超时（＞12 小时），扣 2 分/次
				3	服务期内三级故障解决时间超时（＞24 小时），扣 0.5 分/次
				3	服务期内四级故障解决时间超时（＞48 小时），扣 0.3 分/次
2	运维服务质量与履约情况（30 分）	基础运维服务履约情况	15	5	未按合同约定提供运维服务，出现推诿、拖延、拒绝服务的情况，扣 1 分/次，扣完为止
				5	日常运维工作记录、故障处置记录、巡检记录不完整、虚报、篡改的，扣 1 分/次，扣完为止
				5	未按时提交运维月报、季报、年报及专项报告的，扣 1 分/次，扣完为止
		数据库专项运维服务质量	10	2	未按要求完成月度数据库巡检，少 1 次扣 0.5 分，扣完为止
				2	未按要求完成数据库优化、备份恢复演练的，扣 1 分/次，扣完为止
				2	未及时修复数据库高危漏洞的，扣 1 分/次，扣完为止
				2	数据库运维记录不完整、问题处置不及时的，扣 0.5 分/次，扣完为止
				2	未按要求提供数据库迁移、数据

					备份服务的，扣 0.5 分/次，扣完为止
		系统接口与报表服务质量	5	3	系统接口、报表问题响应不及时、处置不到位的，扣 1 分/次，扣完为止
				2	因政策变化需调整接口、报表、上报规则，未及时完成适配更新的，扣 2 分/次，扣完为止
3	系统升级与合规服务（8 分）	系统升级与补丁更新服务	5	2	未成立升级服务专班、组织架构不合理、技术能力不达标，扣 2 分
				3	未按要求完成系统安全补丁更新、政策合规适配升级，升级过程出现重大故障、影响业务的，扣 3 分
		升级服务质量	3	1	升级服务日志、测试报告、实施方案等资料不完整的，扣 1 分/次，扣完为止
				2	升级后出现遗留问题、使用部门评价达标率＜90%的，扣 1 分/次，扣完为止
4	网络与数据安全服务（25 分）	网络安全与等保合规服务	10	1	未成立安全整改专班、未按等保测评要求制定整改方案的，扣 1 分
				6	未按要求完成等保测评问题整改、整改不及时不到位的，扣 2 分/次，扣完为止
				3	未配合医院完成等保复测，或复测达标率＜80%的，扣 3 分
		数据安全服务	10	2	未建立数据安全保护机制、未提供数据安全合理化建议的，扣 2 分
				8	未通过技术方案保障采购人数据安全，出现数据安全隐患未及时处置的，扣 2 分/次，扣完为止
		数据信息保密管理	5	1	未建立保密管理制度、保密机制不健全的，扣 1 分
				2	未与采购人、项目服务人员签订保密协议的，扣 1 分/项
				2	未制定保密相关考核制度、人员管理不到位的，扣 1 分

		重大安全事件否决项	-	-	发生信息泄露、重大数据安全事件的，本大项 20 分全部扣除，同时直接认定年度考核不合格，追究对应违约责任
5	培训服务（5 分）	培训服务履约与质量	5	2	未按合同要求制定培训计划、编制培训教材的，扣 2 分
				3	未完成年度培训学时要求，少 1 学时扣 1 分；培训后考核不达标、培训效果未达要求的，扣 1 分/次，扣完为止
6	配套设备运维服务（2 分）	设备运维服务质量	2	2	未按合同要求提供配套设备运维服务、工作记录不完整的，扣 1 分；服务期内设备故障率＞10%的，扣 1 分，扣完为止
7	服务满意度与项目管理（5 分）	服务满意度	3	3	服务满意度＜90%的，扣 3 分；发生重大服务质量投诉的，本项 3 分全部扣除
		项目管理评价	2	2	采购人信息科、质控科对服务商项目管理、协调能力评价不合格的，本项 2 分全部扣除
合计	-	-	100	100	-