

陕西省康复医院网络信息安全等级 保护测评项目

合 同

合同编号：SKFY-CGH-X-F2025-12

甲方：陕西省康复医院

乙方：西安捷润数码科技有限公司

签订日期：2025 年 12 月 31 日

需方(甲方): 陕西省康复医院

地 址: 西安市雁塔区电子二路 52 号

电 话: 029-88262021

邮 编: 710065

供方(乙方): 西安捷润数码科技有限公司

地 址: 西安市高新区科技二路 72 号捷普大厦四楼

电 话: 029-89851130/18992875236

邮 编: 710075

联 系 人: 罗杨奕

签约地点: 西安市雁塔区

根据《中华人民共和国民法典》的规定和甲方需求,本着平等互利、协商一致的原则,经甲乙双方友好协商,特订立本合同,共同遵守。

第一条 标的物清单

(一) 项目名称: 网络信息系统安全等级保护测评项目

(二) 项目实施地点: 陕西省康复医院指定地点

(三) 项目范围:

本项目负责完成陕西省康复医院 2025 年度网络安全等级保护测评服务和其它网络安全保障服务,等级保护测评服务包括定级、备案和测评等服务,从“安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理”等方面开展等级保护测评工作,测评对象为 7 个三级信息系统“医院综合信息系统、电子病历系统、医学影像信息系统(PACS)、陕西省康复医院患者服务平台、心电网络系统、DRG 管理及医保智能审核系统、传染病智能监测预警前置软件”,1 个二级信息系统“OA 办公系统”;其它网络安全保障服务包括:应急响应及应急处理服务、重要时期保障服务、安全巡检服务、安全培训服务。

(四) 项目内容:自本协议签定之日起,乙方提供以下服务。

① 网络安全等级保护测评服务

依据《基本要求》(GB/T 22239-2019)、《测评要求》(GB/T 28448-2019)和《测评过程指南》(GB/T 28449-2018)等国家关于网络安全等级保护 2.0 的相关

标准和规范要求，为医院提供以上 7 个信息系统等级保护测评实施工作，测评工作包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理 10 个层面测评。在开展网络安全等级保护测评工作过程中要求严格遵循如下流程：

a、定级备案：按照等级保护相关制度要求，本着自主定级的原则，协助医院完成未备案信息系统的定级报告编制、备案表填写，组织相关专家对定级结果进行评审，完善相关资料，递交至公安部门完成定级备案工作。

b、系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状，出具《资产调查表》。

c、现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果，出具《现场检查表单》。

d、分析整改：分析信息系统安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合医院安全整改工作，出具《整改建议书》。

e、等级测评：根据差异化测评以及国家等级测评相关标准及编制的相关等级保护测评指导书进行符合性测评，并进行记录。

f、结论报告（报告编制）：分析当前信息系统安全保护能力是否符合二级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关信息系统测评报告。

g、配合验收：整理项目过程中所有相关的过程文档，提交医院。按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

② 重大事件应急响应及应急处理服务

在项目服务期内，提供 7×24 小时的信息安全应急处理保障服务。一旦信息系统出现紧急重大安全事件，收到陕西省康复医院的服务请求，测评单位自接到通知 10 分钟内响应，在 2 小时内到达现场，成立应急小组对信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。完成技术服务后需提供相应的《应急响应及应急处理报告》。

③ 重要时期保障服务

在项目服务期内，根据医院实际需要，为医院提供在国家重大政治活动和节假日期间的技术防护保障服务，针对近期可能发生的网络安全威胁，提供技术防护服务，确保活动期间的网络安全可靠运行。

④ 安全巡检服务

在项目服务期内，为医院提供至少每季度 1 次的安全巡检服务，对所有软硬件设备、信息系统进行深度安全巡检，包括但不限于对信息系统中指定的服务器、网络设备、安全设备及安全日志等的安全状态核查。摸清被测系统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行安全检查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策并协助医院进行风险问题整改。每月提供一次风险预警报告，如因巡查不及时，未检查出风险项目而被上级和网监部门通报，扣除本季度巡检服务费的 10%。

⑤ 安全培训服务

在项目服务期内，为医院提供每季度 1 次的信息安全相关专业知识培训服务，包含网络安全意识培训及网络安全技术培训，网络安全意识培训内容主要包括：网络安全法知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训。安全技术能力培训针对主机安全、应用安全、网络安全、数据库安全相关的检查方法进行培训。结合医院实际情况，每季度制定一份为全院职工关于网络安全方面的培训内容。

⑥ 制度体系建设服务

在项目服务期内，协助医院建立网络安全管理制度，完善网络安全管理机构部门岗位职能，落实安全责任；协助解决信息系统安全方面存在的技术问题，提高信息系统安全保障水平，保证信息系统安全稳定运行；构建基础的网络安全管理体系，并分类整理相关制度资料、形成胶装文件、电子档案以及管理制度展板制作。

（五）合同总价款：人民币（小写）209000 元，大写：¥贰拾万零玖仟元。

说明：本合同为一次性包死，不受市场价格变化因素的影响。

第二条 服务标准

对应《信息安全技术网络安全等级保护基本要求》各安全要求项的测评称为单项测评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象实施的综合安全测评。具体测评项如下表：

三级系统测评指标

安全层面	安全子类	测评指标描述
安全物理环境	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；
		b) 应将通信线缆铺设在隐蔽安全处；
		c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地；
		b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
		b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
		c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
		c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
	防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施；
		b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备；
		b) 应提供短期的备用电力供应，至少满足设备在断电

安全层面	安全子类	测评指标描述
		情况下的正常运行要求；
		c) 应设置冗余或并行的电力电缆线路为计算机系统供电。
	电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰；
		b) 应对关键设备实施电磁屏蔽。
安全通信网络	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要；
		b) 应保证网络各个部分的带宽满足业务高峰期需要；
		c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
		e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a) 应采用校验技术或经国家密码局认证核准的密码技术保证通信过程中数据的完整性；
		b) 应采用国家密码局认证核准的密码技术保证通信过程中数据的保密性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
		b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制；
		c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制；
		d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
		b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
		d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
		e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

安全层面	安全子类	测评指标描述
	入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
		b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
		c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
		d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
		b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
	安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具体要求包括： 1) 系统应为不同用户提供不同的用户身份标识； 2) 系统的用户名和口令不得相同，用户口令应为数字、字母、特殊字符混合组合； 3) 用户口令长度应不低于 8 位； 4) 系统应具有用户口令定期更新提示和更新确认； 5) 禁止明文存储口令。
		b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，具体要求包括： 1) 宜限制操作系统同一用户连续登录失败次数为 6-10 次，具体次数应在相关安全策略中明确； 2) 登录失败超过规定次数，用户账户应被锁定 10 分钟，或申请由系统管理员进行密码重置。

安全层面	安全子类	测评指标描述
		c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，具体要求包括： 应采用 SSH、Https、VPN 等安全的远程管理方式。
		d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用国家密码局认证核准的密码技术来实现，具体要求包括： 其中一种鉴别技术宜采用动态口令、数字证书、生物特征或设备指纹。
	访问控制	a) 应对登录的用户分配账户和权限；
		b) 应重命名或删除默认账户，修改默认账户的默认口令，具体要求包括： 操作系统应禁用无法重命名或无法删除的默认账户，或阻止默认账户直接远程登录。
		c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
		e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
	安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d) 应对审计进程进行保护，防止未经授权的中断。
	入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b) 应关闭不需要的系统服务、默认共享和高危端口；
		c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
		e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
		f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码	应采用免受恶意代码攻击的技术措施或主动免疫可信

安全层面	安全子类	测评指标描述
	防范	验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	a) 应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
		b) 应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	a) 应采用国家密码局认证核准的密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
		b) 应采用国家密码局认证核准的密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；
		b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
		c) 应提供重要数据处理系统的冗余，保证系统的高可用性。
	剩余信息保护	a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
		b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；
		b) 应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a) 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b) 应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录

安全层面	安全子类	测评指标描述
		进行存储、管理和查询等。
	安全管理	a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
		b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
	集中管控	a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
		b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
		c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
		d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
		e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a) 应对安全管理活动中的各类管理内容建立安全管理制度；
		b) 应对管理人员或操作人员执行的日常管理操作建立操作规程；
		c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定； b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
安全管理机构	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		c) 应设立系统管理员、安全审计员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	a) 应配备一定数量的系统管理员、安全审计员和安全

安全层面	安全子类	测评指标描述
		管理员等；
		b) 应配备专职安全管理员，不可兼任。
	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
		c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
		b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
		c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
安全管理 人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用；
		b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
		c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
		b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
		c) 应定期对不同岗位的人员进行技能考核。
	外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c) 外部人员离场后应及时清除其所有的访问权限；

安全层面	安全子类	测评指标描述
		d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c) 应保证定级结果经过相关部门的批准；
		d) 应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含国家密码局认证核准的密码技术的相关内容，并形成配套文件；
		c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定，具体要求包括： 应根据党政机关电子公文系统安全可靠应用推进工作领导小组办公室发布的安全可靠应用相关产品目录采购产品。
		b) 应确保密码产品与服务的采购和使用符合国家密码管理局的要求；
		c) 应预先对产品进行选型测试，确定产品的候选范围，并及时审定和更新候选产品名单，具体要求包括： 应按照党政机关电子公文系统安全可靠应用推进工作领导小组办公室相关工作要求进行产品选型测试。
		d) 应通过专有的应用供应渠道下载软件。
	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
		e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
		f) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
		g) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

安全层面	安全子类	测评指标描述
	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码;
		b) 应保证开发单位提供软件设计文档和使用指南;
		c) 应保证开发单位提供软件源代码, 并审查软件中可能存在的后门和隐蔽信道。
	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理;
		b) 应制定安全工程实施方案控制工程实施过程;
		c) 应通过第三方工程监理控制项目的实施过程。
	测试验收	a) 应制订测试验收方案, 并依据测试验收方案实施测试验收, 形成测试验收报告;
		b) 应进行上线前的安全性测试, 并出具安全测试报告, 安全测试报告应包含密码应用安全性测试相关内容。
	系统交付	a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点;
		b) 应对负责运行维护的技术人员进行相应的技能培训;
		c) 应提供建设过程文档和运行维护文档。
	等级测评	a) 应定期进行等级测评, 发现不符合相应等级保护标准要求的及时整改;
		b) 应在发生重大变更或级别发生变化时进行等级测评;
		c) 应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定; 具体包括: 应按照党政机关电子公文应用推进工作领导小组办公室的要求和服务商推荐名录选择服务供应商, 如集成服务、软件开发等单位;
		b) 应与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务;
		c) 应定期监督、评审和审核服务供应商提供的服务, 并对其变更服务内容加以控制。
安全运维管理	环境管理	a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;
		b) 应建立机房安全管理制度, 对有关物理访问、物品带进出和环境安全等方面的管理作出规定;
		c) 应不在重要区域接待来访人员, 不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	a) 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容;
		b) 应根据资产的重要程度对资产进行标识管理, 根据资产的价值选择相应的管理措施;

安全层面	安全子类	测评指标描述
		c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
		b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
		b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
		c) 信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
		d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
		b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
	网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
		f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
		h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

安全层面	安全子类	测评指标描述
		i) 应严格控制远程运维的开通, 经过审批后才可开通远程运维接口或通道, 操作过程中应保留不可更改的审计日志, 操作结束后立即关闭接口或通道;
		j) 应保证所有与外部的连接均得到授权和批准, 应定期检查违反规定无线上网及其他违反网络安全策略的行为。
	恶意代码防范管理	a) 应提高所有用户的防恶意代码意识, 对外来计算机或存储设备接入系统前进行恶意代码检查等;
		b) 应定期验证防范恶意代码攻击的技术措施的有效性。
	配置管理	a) 应记录和保存基本配置信息, 包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等;
		b) 应将基本配置信息改变纳入变更范畴, 实施对配置信息改变的控制, 并及时更新基本配置信息库。
	密码管理	a) 应遵循密码相关国家标准和行业标准;
		b) 应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	a) 应明确变更需求, 变更前根据变更需求制定变更方案, 变更方案经过评审、审批后方可实施;
		b) 应建立变更的申报和审批控制程序, 依据程序控制所有的变更, 记录变更实施过程;
		c) 应建立中止变更并从失败变更中恢复的程序, 明确过程控制方法和人员职责, 必要时对恢复过程进行演练。
	备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等;
		b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等;
		c) 应根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;
		b) 应制定安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等;
		c) 应在安全事件报告和响应处理过程中, 分析和鉴定事件产生的原因, 收集证据, 记录处理过程, 总结经验教训;
		d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
	应急预案	a) 应规定统一的应急预案框架, 包括启动预案的条件、

安全层面	安全子类	测评指标描述
	管理	应急组织构成、应急资源保障、事后教育和培训等内容；
		b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
		c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
		d) 应定期对原有的应急预案重新评估，修订完善。
	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；
		b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
		c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
		d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

第三条 付款方式和条件

(一) 等保测评服务费

1. 服务费¥(大写:)贰拾万零玖仟元/年。
2. 合同有效期为 2025 年/12月21日至 2026 年/12月31日
3. 服务期限：服务期一年。
4. 服务人员数量及组成：

(1) 测评人员要求：本项目的测评人员需具有 1 年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，确保人员稳定，如需更换测评人员，须由医院同意。

(2) 人员配备：乙方参与此项目不少于 6 人，现场测评人员不得少于 4 人，其中至少包含 1 名高级测评师，2 名中级测评师。乙方必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。

(3) 乙方应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

(二) 验收与付款方式

1. 验收方式

项目交付物：①《信息系统安全等级保护测评方案》；②《信息系统安全等级测评报告》；③《信息系统整改建议书》；④《信息系统渗透测试报告》；⑤《信息系统安全等级保护定级备案证明》

验收方式：甲方以会议形式，根据合同、招标文件、验收资料等文件，组织项目验收。乙方出具的报告、方案、建议书等交付物，其内容深度、技术结论及合规性应满足国家相关标准及公安机关等级保护备案的实质性要求。其中，《信息系统安全等级保护测评报告》须具备通过公安机关备案审查的完备性，若因报告本身质量问题导致备案失败或产生额外修改费用的，由乙方承担全部责任。

2. 付款方式

合同签订后支付合同总金额的 30%，甲方收到项目交付物并验收通过及乙方开具的正式发票后，支付合同总金额的 40%。甲方每季度收到供应商巡检报告，按季度支付合同总金额的 7.5%，直至服务结束支付完成。季度考核不合格的，甲方有权扣减直至拒绝支付当季款项。

(三) 支付方式

通过银行转帐方式将款项转入乙方银行帐户。

乙方银行帐户信息如下：

帐户名称：西安捷润数码科技有限公司

帐号：611301134018010089621

开户行：交通银行西安高新区科技支行

甲方仅认可上述指定账户并向该账户付款。如乙方账户信息变更，乙方应出具由法定代表人签署的书面变更文件并加盖乙方公司公章，否则甲方有权拒绝向指定账户之外的任何账户付款，并且由此导致的付款延迟责任由乙方承担。

(四) 结算要求：

乙方要如实开具发票，不得变更开票内容，乙方开具发票出现税务争议时乙方需承担税款、滞纳金、罚款等赔偿责任以及其他相关责任。乙方迟延开具发票、无法开具发票或开具的发票金额低于约定金额的，甲方有权相应地迟延付款、暂不付款或按低于约定金额的发票金额来付款，并对此不承担任何责任。

第四条 其他

1. 为期一年的售后服务工作中，乙方将向医院提供包括应急响应及应急处理

服务、配合检查服务、电话支持服务、安全咨询服务等服务在内的安全维保服务。具体服务内容如下：

（1）应急响应及应急处理服务

针对本次项目，乙方提供 7×24 的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话 10 分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

（2）配合检查服务

乙方根据院方需要，无条件协助医院响应配合公安部、网信办等信息安全监管部门的安全检查工作，按照安全检查的各项要求，并配合开展安全自查。

（3）电话支持服务

乙方提供每周 7 天/每天 24 小时不间断的电话支持服务，解答医院在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过 10 分钟，到达现场时间不超过 2 小时，解决问题不超过 24 小时。

（4）安全咨询服务

乙方为医院无条件提供一年技术咨询服务，提供每周 7 天*24 小时不间断的电话支持服务，解答客户遇到的网络安全问题，及时提出解决问题的建议和操作方法，帮助客户解决信息安全相关技术问题。

（5）安全巡检服务

乙方为医院无条件提供一年安全巡检服务，并每季度提供巡检报告，摸清被测系统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行开展自查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策。每月提供一次风险预警报告，提供最新的风险预警信息。

（6）安全培训服务

为建立人才培养机制，通过网络安全教育，提升全员网络安全防范意识和法

律意识，提升技术支撑服务队伍和网络安全员网络安全处置能力，提高应对突发网络与信息安全事件的综合能力。乙方为医院信息化技术人员提供信息安全相关专业技术知识培训。要求每季度无条件为客户提供一次培训，并提供最新网络风险预警报告。

2. 保密声明

双方确定因履行本合同应遵守的保密义务和责任声明如下：

2.1) 甲方的义务和责任：

2.1.1) 保密内容(包括技术信息和经营信息)：乙方的工作方式、原理，以及竞争性技术、工作成果。

2.1.2) 涉密人员范围：甲方的所有项目人员

2.1.3) 保密期限：不论本合同是否变更、解除、终止，长期有效。

2.1.4) 泄密责任：赔偿乙方因泄密造成的经济损失，直至追究法律责任。

2.2) 乙方的保密义务和责任：

2.2.1) 保密内容(包括技术信息和经济信息)：甲方网络设备、信息系统、信息数据等相关信息、本合同服务范围内的工作成果。

2.2.2) 涉密人员范围：乙方的所有项目人员

2.2.3) 保密期限：不论本合同是否变更、解除、终止，长期有效。

2.2.4) 泄密责任：赔偿甲方因泄密造成的经济损失，直至追究法律责任。

根据以上声明，乙方的所有涉密人员需与甲方单位签订专门的保密协议。

第五条 违约责任

1. 服务缺陷的补救措施和索赔

(1) 如果乙方提供的服务不符合本合同约定以及磋商文件、响应文件关于服务的要求和承诺，乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜：

①乙方同意将服务款项退还给甲方，由此发生的一切费用和损失由乙方承

担。如甲方以适当的条件和方法购买与未履约标的相类似的服务，乙方应负担新购买类似服务所超出的费用。

②根据服务的质量状况以及甲方所遭受的损失，经过甲乙双方商定降低服务的价格。

(2)如果在甲方发出索赔通知后 10 日内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后 10 日内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付服务款中扣除索赔金额或者没收履约保证金，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

2. 未履行合同义务的违约责任

(1)守约方有权终止全部或部分合同。

(3)由违约一方支付合同总金额 20%的违约金。

(3)违约金不足以弥补守约方实际损失、可预见或者应当预见的损失，由违约方全额予以赔偿。

(4)依据《中华人民共和国民法典》、《中华人民共和国政府采购法》的相关条款和本合同约定，乙方未全面履行合同义务或者发生违约，甲方会同采购代理机构有权终止合同，依法向乙方要求经济索赔，并报请政府采购监督管理机关进行相应的行政处罚。若乙方出现以下情形之一，视为根本违约，甲方有权单方解除合同，并要求乙方支付合同总金额 20%的违约金，违约金不足以弥补甲方全部损失的（包括但不限于直接损失、预期利益损失、为实现权利支出的律师费、诉讼费等），乙方应继续赔偿：

①交付的《信息系统安全等级保护测评报告》存在重大错误、遗漏或不符合国家标准，导致无法通过公安机关备案，且在甲方要求期限内修改后仍无法通过的；

②未经甲方书面同意，擅自更换项目经理或高级测评师，或项目团队人员不足，严重影响项目进度或服务质量的；

③违反保密义务，泄露甲方系统数据、网络拓扑等敏感信息，造成实际损害的；

④无正当理由，迟延交付关键工作成果超过 30 日的。

(5) 甲方违约的，应当赔偿给乙方造成的经济损失。

(6) 延迟交付:如因乙方自身原因导致未能如期交付工作成果，则每延期_1_日，应向甲方支付应付款项的 0.5%作为违约金。

第六条 争议处理

本合同在履行过程中发生的任何争议，应由甲、乙双方友好协商解决，协商不成的，甲乙双方任意一方有权向甲方所在地人民法院提起诉讼。因违约方违反约定事宜产生纠纷，守约方由此产生的费用（包括但不限于诉讼费、律师费、保全费、保全保险费）均由违约方承担。

第七条 甲乙双方的权利义务

1. 甲方的权利义务：1) 甲方有权对合同约定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分有权下达整改通知书，并要求乙方限期整改。2) 负责检查监督乙方管理工作的实施及制度的执行情况。3) 根据本合同约定，按时向乙方支付应付服务费用。4) 国家法律、法规所规定由甲方承担的其它责任。

2. 乙方的权利和义务：1) 按本合同约定的服务内容向甲方提供全面服务，并对甲方提出的合理要求进行响应。2) 根据本合同的约定向甲方收取相关服务费用，并有权在本项目管理范围内管理及合理使用。3) 及时向甲方通告本项目服务范围内有关服务的重大事项，及时配合处理投诉。4) 接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。5) 国家法律、法规所规定由乙方承担的其它责任。

3. 甲方责任：

3.1 按合同规定提供予以项目便利的配合，包括及时提供准确完整的相关资料、办公环境和网络环境。

3.2 负责协调乙方工作过程中与本项目有关科室的配合问题。

4. 乙方责任：

4.1 乙方应根据合同的规定，在双方约定的时间内完成服务项目内容。

4.2 乙方应根据工作需要，派出相关专业的工作人员进行项目配合及监督执行。

4.3 乙方应按国家规定和本合同及采购文件约定的服务规范和要求进行服

务，并对服务质量负责。

第八条 不可抗力

1. 如果合同双方因不可抗力而导致合同实施延误或合同无法实施，不应该承担误期赔偿或不能履行合同义务的责任。

2. 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

3. 在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可抗力事件结束后3日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行的协议。

第九条 履约说明

乙方在合同服务期内，须完全履行磋商文件、响应文件及合同中的服务要求、承诺内容和售后服务，未完全履行的，则视为虚假应答，将乙方纳入失信名单。

第十条 其他约定

本协议中未涉及的事项，双方本着公平公正原则，友好协商解决，补充协议与本协议具有同等法律效力。

第十一条 合同生效

本合同一式肆份，甲方执叁份、乙方执壹份，自甲乙双方签字、盖章之日起生效，各份合同均具有同等法律效力。

(以下无正文)

(签署页)

甲方（公章）

单位名称：陕西省康复医院

法定代表人或授权代表：

（签字）



王琳

联系电话：029-88262021

签订日期：2025 年 12 月 31 日

乙方（公章）

单位名称：供方(乙方)：西安捷润数码科
技有限公司

法定代表人或授权代表：

（签字）



张红

联系电话：

18992875236

签订日期：2025 年 12 月 31 日

附件 1:

廉洁协议书

甲方（医疗机构）：陕西省康复医院

乙方（供应商）：西安捷润数码科技有限公司

为深入贯彻落实中省卫生系统纪检监察暨纠风工作会议精神，进一步加强医疗卫生行风建设，规范药品、医疗器械、医用卫生材料等产品购销行为，有效防范商业贿赂行为，营造公平交易、诚实守信的购销环境，维护正常的医疗秩序和医药产品经营秩序，建立健全防治商业贿赂长效机制，经甲、乙双方协商，同意签订本协议书并予以共同遵守：

一、甲、乙双方按照《中华人民共和国民法典》及合同约定购销产品。

二、甲方在采购货物、服务、工程项目过程中，不得以任何方式向乙方索取回扣，或者索要、收受乙方产品发票价外的赞助，不得要求乙方代支任何费用开支。

三、甲方工作人员不得以暗示或其他任何形式索要回扣、提成、有价证券、现金、购物卡等。如甲方工作人员暗示或索要，乙方应予拒绝，并有责任如实向甲方纪检监察部门反映情况。

四、甲方工作人员不得替乙方非法统计药品、耗材销售数量等有关信息。

五、乙方不得暗中给予甲方回扣，不得以提成和赠送有价证券、现金、购物卡、宴请、娱乐及提供国内或境外学术活动旅游、超标准支付食宿费用等手段影响甲方医生使用医药器械等产品的选择权。

六、乙方洽谈业务，必须在工作时间到甲方指定科室联系商谈，遵守院内医药代表院内拜访管理制度，至行风办进行预约登记，不得到临床、门诊等推销产品，不得借故到甲方相关领导、部门负责人及相关工作人员家中访谈或向介绍人提供任何好处费。

七、乙方在销售活动中，要自觉遵守国家和地方的有关法律、法规，严格执行合同条款，不以次充好，不降低产品质量，做到诚信经营。

八、乙方如违反本协议条款，一经发现，甲方有权终止购销合同，并向有关卫生计生行政部门或政府采购监管部门报告。该行为列入不良行为记录，并在单位内通报，取消供应商在医院的配送资格 2 年，涉嫌违法的，由执法部门予以处

理。

九、甲方工作人员如违反以上条款的，甲方将按国家有关法律、法规规定和有关廉政制度规定给予处理，涉嫌违法的，由执法部门予以处理。

十、本协议书为购进药品、医疗器械、医用卫生材料等产品合同的附件，与购销合同一并执行，具有同等的法律效力。

十一、本协议作为合同的附件，与合同具有同等法律效力。经双方签署并盖章后立即生效。

甲方（盖章）：

法定代表人/授权代表：

2025 年 12 月 31 日



封彬

乙方（盖章）：

法定代表人/授权代表：

2025 年 12 月 31 日



张银生

