

西安市红会医院
等级保护测评合同

合同编号：X-XXKHT2026225

甲方：西安市红会医院

乙方：西安捷润数码科技有限公司

3. 合同总价一次性包死，不受市场价格、政府政策、不可抗力等变化因素的影响所有费用等。

2. 合同总价包括但不限于：运输费、保险费、装卸费、配套资料费、安装调试费、强制性第三方监督检验机构的验收检验费、培训费用以及售后服务费用及税金等

1. 合同总价款为¥180,000.00元（人民币：壹拾捌万元整）。

二、合同价款

2. 合同期限：自合同签订之日起一年。

序号	测评系统名称	测评系统等级	单价（元）
1	互联网应用系统	三级	50,000.00
2	信息集成平台	三级	50,000.00
3	HIS+EMR	三级	50,000.00
4	门户网站系统	二级	30,000.00
总价			大写：人民币壹拾捌万元整；小写：¥180,000.00元

1. 测评系统名称及单价。

一、合同标的物内容

甲、乙双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》及其他相关法律的规定，就乙方为甲方提供等级保护测评事宜，甲、乙双方经协商一致达成如下协议，并由双方共同遵照执行。

根据国家《信息安全等级保护管理办法》（公通字[2007]43号）与《信息安全技术网络安全等级保护基本要求》GB/T22239-2019等相关文件要求，对西安市红会医院互联网医院系统,信息集成平台,HIS+EMR,门户网站系统实施网络安全等级保护测评工作。

甲方：西安市红会医院（以下简称“甲方”）

乙方：西安捷润数码科技有限公司（以下简称“乙方”）

响，合同履行期间，无论发生任何突发或者其他事件，甲方不再另行支付任何费用。

三、结算方式及账户信息

1. 履约保证金的收取与退回：在中标结果公示发布后 5 个工作日内乙方将项目履约保证金（中标总金额的 5%，即 9,000.00 元）转账至甲方基本户，未按照招标文件要求按时足额缴纳履约保证金的，甲方将取消乙方中标资格，且无需承担任何责任，甲方可重新组织招标活动。合同所约定事宜完成，无任何问题，甲方向乙方无息退还履约保证金。
2. 款项结算：合同签订生效后，乙方按甲方年度工作安排开展信息系统等级保护测评服务。每自然年度内，乙方完成当年甲方指定数量系统的等保测评并全部取得备案证明并经甲方确认（以甲方出具结论为合格的书面验收报告为准），视为当年度测评服务验收合格。

验收合格后，乙方向甲方开具当年实际完成备案系统对应金额 90%的合法合规发票，甲方在收到合规发票后 30 日内，向乙方支付当年度 90%的应付测评款项。剩余 10%的应付测评款项，待乙方完成本项目约定的全部培训内容并经甲方确认后，由乙方向甲方开具剩余款项合法合规发票，甲方在收到合规发票后 30 日内付清尾款。若乙方延期开票，甲方有权暂停付款，不视为甲方违约且无需承担任何责任，乙方应按照合同正常履行义务。如因甲方财务制度及付款流程等原因导致延期支付，双方友好协商解决。

3. 支付方式：银行转账。

4. 甲乙双方银行账户信息和纳税人信息如下：

甲方：西安市红会医院

开户行：[中国银行西安碑林区支行营业部]

银行地址：[陕西省西安市碑林区南关正街 3 号]

户名：[西安市红会医院]

账号：[102407334632]

统一社会信用代码：[12610100437203580Q]

地址：[西安市碑林区南稍门南郭路 76 号]

电话：[029-87800002]

乙方：[西安捷润数码科技有限公司]

开户行：[交通银行西安高新区科技支行]

银行地址：[西安市高新区科技二路 68 号]

户名：[西安捷润数码科技有限公司]

账号：[611301134018010089621]

统一社会信用代码：[91610131726291097U]

地址：[西安市高新区科技二路 72 号捷普大厦四楼]

电话：[029-89851130]

上述账户信息不得变更。

四、服务内容

1. 评测系统等级

(1) 三级包含：互联网医院系统,信息集成平台,HIS+EMR。

(2) 二级包含：门户网站系统。

2. 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。

3. 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。

4. 分析整改：根据前述工作内容，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，配合采购单位安全整改工作。

5. 结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关系统测评报告。

6. 配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员。

五、技术要求

1. 总体要求

根据国家《信息安全等级保护管理办法》(公通字[2007]43号)与《信息安全技术网络安全等级保护基本要求》GB/T22239-2019要求，等级测评工作须覆盖安全物理环境、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的内容，并根据现场实际情况完成风险分析工作，最终为完善等级保护安全防护体系提供指导依据。

2. 第一阶段：等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、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、安全运维管理十个安全类别进行安全测评。

(1) 定级要求

该项工作开展的主要依据是《网络安全等级保护定级指南》(GB/T 22240-2020)确定系统等级。

(2) 备案

信息系统的安保等级确定后，二级以上(含二级)信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国联网运行的信息系统在各地运行、应用的分支机构，向当地设区的市级以上公安机关备案。该项目系统应向属地网络安全监察支队申请重要信息系统备案。完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

3. 等级保护测评要求

服务商在测评过程中要求按照等保相关的标准规范开展等级测评工作，对系统的安全物理环境、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、安全运维管理共 10 个层面进行安全等级保护测评。测评指标如下：

三级等级保护技术要求

层面	控制点	测评项
安全物理环境	物理位置选择	a) 机房和办公场地应选择在有防震、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高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	a) 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，并设置明显的不易去除的标识； 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。

层面	控制点	测评项
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。
		可信验证 a) 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
		通信传输 a) 应采用校验技术或密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中数据的保密性。
	电磁防护	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。
		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。
		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 a) 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。
	防水防潮	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。

层面	安全区域边界	入侵防范	访问控制	边界防护	控制点	测评项
		键执行环节进行动态可信验证，在监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。	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测或限制； 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。	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。	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、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	

层面	控制点	测评项
安全环境	垃圾邮件防 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、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。
安全环境	可信验证	a) 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。
	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; b) 应启用登录失败处理功能,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时自动退出等相关措施; 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; 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密码技术实现。
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;

层面	控制点	测评项
		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。
		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、时间、事件类型、事件是否成功及其他与审计相关的工作; 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。
		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。
	入侵防范	a)应采用免受恶意代码攻击的技术措施,或主动免疫可信验证
	恶意代码防	

层面	控制点	测评项
安全管理中心	范	机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	a) 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。
	数据完整性	a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于数据鉴别、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，包括但不限于数据鉴别、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，包括但不限于数据鉴别、重要业务数据和重要个人信息等；
		b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等。
	数据备份和恢复	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用场地；
		c) 应提供重要数据处理系统的热冗余，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	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。
	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

层面	控制点	测评项
安全管理	审计管理	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。 a) 应对审计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审计操作，并对这些操作进行审计； b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行行处理，包括根据安全审计策略对审计记录进行存储、管理和查询。
		a) 应对安全管理员进行身份鉴别，只允许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识，对主体进行授权，配置安全可信验证策略等。
		a) 应划分特定的管理区域，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、安全代码、补丁升级等安全事项进行集中管理； f) 应能对网络中发生的各类安全事件进行识别报警和分析。
		a) 应制定网络安全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。
	安全策略	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) 应对要求管理人員或操作人員执行的日常管理操作建立操作规程；
	管理制度	
	安全管理	

层面	控制点	测评项
	制定和发布	c) 应形成由安全策略, 管理制度, 操作规程, 记录表单等构成安全管理制度体系。
		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、有效的方式进行发布, 并进行版本控制。
		a) 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。
安全管理机构	岗位设置	a) 应成立指导和管理网络安全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、审计管理员、安全管理员等岗位, 并定义部门及各个工作岗位的职责。
		a) 应配备一定数量的系统管理员、审计管理员、安全管理员等;
	人员配备	b) 应配备专职的安全管理员, 不可兼任。
		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;
	授权和审批	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安全管理部門之间的合作与沟通, 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、

层面	控制点	测评项
安全管 理人员	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、安全配置和安全策略的一致性，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。
		联系人和联系方式等信息。
	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) 应对被录用人的身份、安全背景、专业资格或资质等进行审 查，对其所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。
		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；
	人员离岗	b) 应办理严格的调离手续，并承诺调离后的保密义务方可离 开。
		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。		
安全意识和培训	a) 应在外部人员物理访问受控区域前提出书面申请，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；	
	d) 获得系统访问授权的外部人员签署保密协议，不得进行非授 权管理	

层面	安全管理	控制点	测评项
			a) 应以书面的形式说明保护对象的安全保护等级及确定安全保护等级的方法和理由； 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
	安全建设	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其他级别对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容、并形成配套文件； c) 应组织相关部门和有关安全技术专家对整体安全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； 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主管部门的要求； c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新产品候选名单。
	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；

层面	控制点	测评项
	发	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。
		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面和隐蔽信道。
	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安全测试内容。
		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;
	系统交付	b) 应对负责系统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。
		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;
	等级测评	b) 在发生重大变化或级别发生时进行等级测评;
		c) 应确保测评机构的选择符合国家相关规定。
		a) 应确保服务供应商的选择符合国家的有关规定;
	服务供应商管理	b) 应与选定的服务商签订相关协议,明确整个服务供应链各方需履行的网络安全安全相关义务;

层面	控制点	测评项
安全运维管理	资产管理	a) 应编制并保存与信息系统相关的资产清单, 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; c) 应对信息分类与标识方法做出规定, 并对信息的使用, 传输和存储等进行规范化管理。
	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, 物品带进带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, 不随意放置包含敏感信息的纸质文件和移动介质。
	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进行定期维护管理; 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) 信息处理设备应经过审批才能带离机房或办公地点, 含有储存介质的设备带出工作环境时其重要数据应加密; d) 含有存储介质的设备在报废或重用前, 应进行完全清除或完

层面	控制点	测评项
	漏洞和风险	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。
	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、参数的设置和修改的内容; 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,经过审批后方可改变连接,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,操作结束后应同步配置更新配置信息库; h) 应严格控制运维工具的使用,经过审批后方可接入进行操作,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; i) 应严格控制远程运维的开通,经过审批后方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,操作结束后应立即关闭接口或通道;
	网络安全和系统	
	安全管理	

层面	控制点	测评项
	恶意代码防范管理	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行为。
		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;
	配置管理	b) 应定期验证防范恶意代码攻击的技术措施的有效性。
		a) 应记录 and 保存基本配置信息, 包括网络拓扑结构、各类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;
	密码管理	b) 应将基本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。
		a) 应遵循密码相关国家标准和行业标准;
	变更管理	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。
		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;
	备份与恢复管理	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) 应建立终止变更并从未失败的变更中恢复的程序, 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。
	安全事件处置	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;

安全层面	安全控制点	测评指标
安全物理环境	物理位置选择	a) 机房场地应选择具有防震、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高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	a) 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴

二级等级保护技术要求

层面	控制点	测评项
	应急管理	a) 应规定统一的应急预案框架，包括启动预案的条件，应急组织机构，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。
	应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件，应急组织机构，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。

安全层面	安全控制点	测评指标	制	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 标记； b) 应将通信线缆铺设在隐蔽安全处； a) 应将各类机柜、设施和设备等通过接地系统安全接地。
	防雷击	a) 机房应设置火灾自动消防系统，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；		
	防火	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。		
	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。		
	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情况下的正常运行要求。		
	电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰。		
	网络	网络架构	a) 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； b) 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。	
		通信传输	a) 应采用校验技术保证通信过程中数据的完整性。	

安全层面	安全控制点	测评指标	可信验证	可信验证	边界防护	访问控制	入侵防范	恶意代码防范	安全审计	可信验证
			a) 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。		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。	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对进出数据流提供明确的允许/拒绝访问的能力；	a) 应在关键网络节点处监视网络安全攻击行为。	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。	a) 应在网络边界、重要网络节点处进行安全审计，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。	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，并在检测到其可

安全层面	安全控制点	测评指标
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； 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； 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。
	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； 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。
	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。
	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；
		信任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。

安全层面		安全管理中心																									
安全控制点	测评指标	恶意代码防范			可信验证			数据完整性			数据和备份恢复			剩余信息保护		个人信息保护		系统管理			审计管理						
		a) 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。			a) 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。			a) 应采用校验技术保证重要数据在传输过程中的完整性。			a) 应提供重要数据的本地数据备份与恢复功能；			b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。			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。		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。		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配置、系统加载和启动、系统管理，包括用户身份、系统资源配置、系统加载和启动、系统运行、异常处理、数据和设备的备份与恢复等。	

安全层面	安全控制点	测评指标	b) 应通过审计管理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进行存储、管理和查询等。	安全管理	制度			安全管理机构				
					安全策略	管理制度	制定和发布	评审和修订	岗位设置	人员配备	授权和审批	
					应制定网络安全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。	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) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程。	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。	a) 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。	a) 应设立网络安全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; b) 应设立系统管理员、审计管理员和安全管理等岗位, 并定义部门及各个工作岗位的职责。	a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。	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执行审批过程。	

安全层面	安全控制点	测评指标	沟通和合作				审核和检查				人员				安全管理	安全管理	安全建设
			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。	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。	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。	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。	a)应对各类人员进行安全意识教育和岗位技能培训,并告知相关的安全生产责任和惩戒措施。	a)应在外部人员物理访问受控区域前提出书面申请,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。	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;			

安全层面		安全控制点	测评指标
		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进行安全方案设计；
			c) 应组织相关部门和有关安全专家对安全方案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) 应确保网络安全安全产品采购和使用符合国家的有关规定；
			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主管部门的要求。
		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。
		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。
		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。
		测试验收	a) 应制定测试验收方案，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。
		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；

安全层面		安全控制点		测评指标																																																																																																																																																																																																																																																																																																																																																																																																																																																									
	安全运维管理	等级测评	服务供应商选择	环境管理	资产管理	介质管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理	安全运维管理

安全层面	安全控制点	测评指标
安全运维管理	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;
	理	b)应对配套设施、软硬件维护管理做出规定,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。
	漏洞和风险	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。
	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;
	网络 and 系统	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;
安全运维管理	安全管理	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。
		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)应对恶意代码防范要求做出规定,包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等;
安全运维管理	恶意代码防范	c)应定期检查恶意代码库的升级情况,对截获的恶意代码进行及时分析处理。
	管理	

安全层面		安全控制点	测评指标					
	配置管理	应记录 and 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。					
		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	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。				
		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；						
	备份与恢复管理	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。				
		a) 应及时向安全管理部門报告所发现的安全弱点和可疑事件；						
		安全事件处置			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。		
					应急预案管理		a) 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；	b) 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。
							外包运维管理	

安全层面	安全控制点	测评指标
		运维的范围、工作内容。

4. 第二阶段：渗透检测

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

5. 第三阶段：建设整改咨询及安全加固（不涉及硬件）

(1) 建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息安全系统安全建设整改建议》将信息系统的建设整改需求落实到可操作的安全技术和管理的上，提出能够实现的技术参数或制度及其具体规范。

(2) 在甲方依据相关《信息安全系统安全建设整改建议》开展建设整改工作，乙方将提供建设整改过程中的与建设整改相关的咨询服务。

(3) 对信息安全系统安全建设整改建议进行确认，并依照建议，协助甲方进行漏洞修复，补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，然后协助甲方分步实施安全整改工作。

六、服务要求

1. 测评人员要求：本项目的测评人员需具有2年或2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，并确保人员稳定。如需更换测评人员，须由甲方同意。

2. 人员配备：参与此项目不少于8人，现场测评人员不得少于6人，其中至少包含2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，能容易地与甲方沟通，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. 针对本项目要保证渗透测试服务质量，提供渗透过程中的风险防范措施和应

应急响应措施。

4. 售后服务

验收之日起为期一年的售后服务，乙方将甲方提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下：

(1) 应急响应服务

针对本次项目，乙方提供 7X24h 的常规应急响应及灾难恢复专家服务。在接到甲方故障报修电话 10 分钟内响应。对甲方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

乙方免费协助甲方响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助甲方准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

(3) 电话支持服务

每周 7 天/每天 24 小时不间断的电话支持服务，解答甲方在使用过程中遇到的问题，及时提出解决问题的建议和方法。电话响应时间不小于 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

乙方为甲方免费提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到甲方的服务请求，乙方技术服务工程师将立即开始提供服务，帮助甲方解决信息安全相关技术问题，全面配合甲方做好业务系统安全保障工作。

(5) 重保支持服务

在重大节假日或活动期间，提供安全技术支持，保障客户相关网站及重要信息系统的安全稳定运行，避免出现信息系统中被非法篡改、挂马等安全事件发生，根据预设应急响应流程进行安全事件处置，最大限度地减少安全事件造成的损害，降低应急处置的风险。提供已发生安全事件的事中、事后的取证、分析及提供解决方案等服务；重保服务包括但不限于以下安全事件的保障服务：应用服务瘫痪；网络阻塞、DDoS

攻击；服务器遭劫持；恶意入侵、黑客攻击；病毒爆发；内部安全事故。

(6) 协助更新备案系统

在项目服务过程中需协助甲方完成旧系统在公安机关注销工作及新系统备案工作（配合甲方准备相关资料），完成相关流程。

(7) 其他扫描服务

配合甲方对指定系统进行深度渗透测试，找出系统中相关的漏洞问题（至少5个系统）。

(8) 合同签订之日起2个月内完成测评工作并提交测评交付物。

七、交付成果

1. 《信息系统安全等级保护定级备案证明》

2. 《信息系统安全等级测评报告》

3. 《信息系统安全建设整改建议书》

八、验收标准或规范

服务商在测评过程中要求按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术 信息系统安全等级保护实施指南》（GB/T25058-2010）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。

九、违约责任

1. 按《中华人民共和国政府采购法》《中华人民共和国民法典》中的相关条款执行。

2. 乙方未按合同要求履行合同义务，所提供服务质量不能满足合同约定的技术

十二、不可抗力

方式记录，或是以口头或视听方式提供的，其产权归提供方所有。

保密或者专有的所有文件、技术资料、商业信息和软件及其相关的文件，无论以何种

2. 由甲乙任何一方提供或公开标有限制使用或传播的说明或以其他方式表明是

的终止而丧失。

给第三方。由此引起的法律纠纷，由泄露方承担全部责任，且该保密义务不因本合同

1. 甲乙双方均应对本合同内容保守秘密，不经对方同意不得将本合同内容泄露

十一、保密条款

2. 诉讼进行过程中，双方继续履行本合同未涉诉的其他部分。

院起诉。

果双方不能通过友好协商解决争议，则任何一方均可向甲方住所地有管辖权的人民法

1. 所有因本合同引起的或与本合同有关的任何争议通过双方友好协商解决。如

十、争议解决

师费、调查取证费、差旅费、鉴定费等全部费用。

行赔偿，另支付守约方合同总价款 30% 的违约金。本条款所指损失：包括但不限于律

解除通知书到达违约方时解除。给守约方造成损失的，违约方还应当在损失范围内进

违约方以实际行动表示不再履行其义务；守约方有权单方面解除本协议，协议自书面

(2) 违约方未在限期内履行完毕其义务；(3) 违约方明确表示其不再履行其义务；(4)

约方视情况决定是否恢复履行其义务；若 (1) 守约方决定不再恢复本合同项下义务；

要求违约方限期履行，待违约方在守约方规定的合理期限内履行完毕相关义务后，守

3. 在合作期内，一方违反本合同约定，另一方可以视情况中止履行相关义务并

同总价的 30% 为违约金；(3) 请政府采购管理部门对其违约行为进行追究。

用)；(2) 乙方支付甲方违约金，违约金计算方法：以合同总价为基数，支付甲方合

购产生的费用、甲方对第三方的违约损失，以及可能产生的律师费、诉讼费 etc 全部费

追究乙方的违约责任：(1) 乙方赔偿甲方解除本合同的全部损失 (包括但不限于重新采

权解除合同，解除合同书面通知到达乙方之日视为合同已解除，并按以下方式

要求，在约定的条件下，乙方必须无条件更换，提高技术，完善质量，否则，甲方有

1. 不可抗力是指本合同生效后，发生合同订立时不能预见、不能避免、并不能克服的客观情况，如地震、台风、水灾、战争等，致使直接影响本合同的履行或不能按约定的条件履行的情况。

2. 发生不可抗力的一方应立即通知对方，并在十五天内提供不可抗力的详情及将有关证明文件送交对方，且应尽可能减少不可抗力所产生之影响。

3. 发生不可抗力事件时，甲乙双方应协商以寻找合理的解决方法，双方不可放任不可抗力事件损害后果。

4. 经双方确认的不可抗力影响时间，不计入本合同执行时间。本合同期限可根据中止的期限作相应延长，但须双方协商一致，任何一方均不会因此而承担责任。

5. 如不可抗力事件持续三十天时，甲乙双方应友好协商解决本合同是否继续履行或终止的问题。

6. 在发生不可抗力时，双方对各自控制下的设备、资料负有保管责任，对于未受不可抗力影响并且可以继续履行的合同义务应继续履行。

十三、合同生效及其他

1. 在本合同执行过程中，甲乙双方协商签订的补充合同与本合同具有同等法律效力，补充合同与原合同不一致的，以补充合同为准。技术协议、采购文件及其补遗文件、投标文件和有关说明承诺（若有）是本合同不可分割的部分，为本合同的重要内容补充内容，与本合同具有同等法律效力。

2. 除本合同另有约定外，未经甲乙双方书面确认，任何一方不得自行变更或修改本合同。

3. 未尽事宜，双方协商解决。

4. 本合同自双方签字盖章之日起生效；本合同一式伍份，甲方肆份，乙方壹份，每份具有同等法律效力。

(本页无正文，为《西安市红会医院等级保护测评合同》签署页)

甲方（盖章）：西安市红会医院
法定代表人或委托代理人签字：

TZS

经办人：[Signature]

签订日期：2026年 8 月 12 日



乙方（盖章）：西安捷润数码科技有限公司
法定代表人或委托代理人签字：



签订日期：2026年 8 月 12 日