

采购需求与技术要求

一、项目概况

为保障陕西省档案馆数字档案馆系统的安全运行，落实《中华人民共和国网络安全法》《信息安全等级保护管理办法》等国家法律法规要求，结合我单位的实际情况，对 8 个信息平台开展网络安全等级保护测评服务工作（包括定级、备案和测评）；举办网络安全培训讲座 2 次；实施网络安全应急攻防演练（数据泄露方向）1 次。

二、测评系统：

序号	系统名称	网域	评审级别
1	陕西档案信息网	互联网	第三级
2	公共信息服务平台	政务外网	第三级
3	电子文件归档及移交进馆平台	政务外网	第三级
4	档案共享利用管理平台	政务外网	第三级
5	目录中心系统	局域网	第三级
6	协同办公系统	局域网	第三级
7	运维管理系统	局域网	第三级
8	数字档案馆综合管理平台系统	局域网	第三级

三、测评依据

政策法规文件：

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《中华人民共和国网络安全法》

《关于信息安全等级保护工作的实施意见》（公通字【2004】66 号）

《信息安全等级保护管理办法》（公通字【2007】43 号）

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安【2009】1429号）

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安【2010】303号）

《关于印发〈陕西省信息安全等级保护安全建设整改工作指导意见〉的通知》（陕等保办【2011】2号）

《陕西省公安厅重要信息系统和重点网站安全执法检查反馈意见》（陕公网字 检字【2015】713号）

标准规范文件：

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术网络安全等级保护测试评估技术指南》（GB/T 36627-2018）

《信息安全技术网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）

《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）

四、服务总体要求：

1) 测评服务要求：依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）等国家关于网络安全等级保护的相关标准和规范要求，为陕西省档案馆提供相应级别网络安全等级保护测评实施工作，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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评。根据国家标准规范，确保最终通过等保测评。

2) 供应商须服从陕西省档案馆的统一协调，且必须在项目实施期间由供应商派驻有丰富实施经验的信息安全等级保护测评中级及以上测评师为项目实施团队主要负责人和核心成员，全程参与项目实施。

3) 供应商须提供完善的测评实施方案和计划、测评方案，经我单位审核通过后实施，并完成我单位对安全管理制度的补充完善和整理工作，配合对我单位网络安全进行整改测评服务。

4) 供应商须提供完善的实施人员组成、资质及合理的责任及角色划分。

5) 实施过程中严控测评工具的使用，须经过陕西省档案馆项目管理人员审批后才可接入系统进行操作，响应文件中应将所使用的测评工具列表说明，并进行详细描述。

6) 渗透测试服务要求：供应商的渗透测试工程师要模拟恶意黑客的攻击方法，来对陕西省档案馆本次测评信息系统的安全性进行检测评估。供应商应确认攻击时使用的方式、对系统平台的相关要求及可能对系统造成的风险等。渗透测试对系统和网络进行非破坏性质的攻击性测试，尝试侵入系统，获取系统控制权并将入侵的过程和细节产生报告，由此证实系统所存在的安全威胁和风险，及时提示采购方修复安全漏洞，提醒采购方完善安全策略，提升系统安全防护能力。

7) 安全需求分析及设计服务要求：为保障陕西省档案馆重要信息系统的安全防护能力，供应商需对其信息系统提供安全需求分析，并且能对陕西省档案馆的信息系统做安全方案设计，提出有针对性的安全规划方案。

8) 安全培训服务：供应商需提供网络安全讲座 2 次，培训内容包括网络安

全意识、网络安全技术、网络安全政策法规等。

9) 供应商须与我单位签订项目合同、保密协议和现场评测授权书、风险预判告知书， 核实驻场测评师资质与投标时对本项目配备的测评师是否一致。确因工作调配更换测评师，应提前 10 个工作日向陕西省档案馆信息技术处书面报备，并提供更换测评师资质证明。

10) 测评工作完成后，应及时组织专家组进行验收。对整个过程中形成的项目文件进行收集整理，向采购方移交两套齐全、完整的项目档案。

11) 测评结束后，服务方需免费提供整改咨询服务和免费质保服务，并提供为期一年的售后服务，就本项目成果中的具体内容提供解释，提供信息系统等级保护相关工作的技术支持和咨询服务，以帮助陕西省档案馆提高安全防护能力。

12) 供应商需在中标后，协助我馆开展备案资料梳理工作，并协助我馆取得公安部门办理的等级保护备案证。

13) 网络与信息安全信息通报服务要求：供应商需要在测评结束后，提供至少的一年网络信息安全通报服务，要与我馆建立完善的通报和沟通机制，及时按照国家标准提供对应服务。

14) 供应商免费协助陕西省档案馆做好公安机关或第三方机构针对信息系统安全等级保护检查工作。服务内容包括协助采购方准备、完善各类资料文档，配合检查过程中的答疑及技术支持，以及其他现场检查的响应。

15) 参加本次项目的供应商近三年未被国家或省级等级保护测评监管部门通报批评、整改。

## 五、测评原则

### 1) 标准性

在项目实施过程中严格按照 GB/T22239-2019、GB/T28448-2019、GB/T28449-2018、GB/T36627-2018 等标准中规定的评测要求、评测方法等进

行项目实施。

## 2) 客观公正性

在没有偏见和最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方法和过程，实施测评活动。

## 3) 规范行为

严格按照测评指导书的使用规范的测评技术进行测评，准确记录测评证据；不得擅自评价测评结果；不将测评结果复制给非测评人员；对被测单位的敏感信息或工作秘密，在指定场所查看，查看后立即归还。

## 4) 规避风险

充分评估测评可能对被测系统带来的影响，揭示风险，协助开展预防措施规避风险。签订现场测评授权书、保密协议。及时与测评委托单位沟通，从而保证项目执行的效果。

## 5) 结果完善性

测评所产生的结果是在对测评指标的正确理解下所取得的良好判断。在测评实施过程中应当使用正确的方法以确保其满足了测评指标的要求。

## 六、项目成果：

《等级保护测评项目系统测评方案》（每个系统二份）；

《等级保护测评项目系统等级保护整改建议书》（每个系统二份）；

《等级保护测评项目系统等级保护测评报告》（每个系统二份）。

## 七、项目管理要求：

### 1) 项目管理总体要求

供应商应在被陕西省档案馆统一组织协调下，开展好前期调研、现场实施和报告撰写等工作。测评机构所提供的项目经理和实施人员应是具有丰富经验和专业技能的技术骨干，应有同类项目经验。在测评机构以往参与的项目中，

应具有项目实施、熟悉项目需求和团队建设方面的优势。测评机构应在项目全过程中严格遵循各项管理制度的要求，确保项目顺利开展。

本项目测评驻场人员要求：本次等保测评服务不得转包或者分包，所有驻场测评师必须是测评机构的正式在职员工，所有驻场测评师必须持证上岗，响应文件中应提供项目组驻场人员名单以及社保主管部门出具的响应单位为其缴纳社保的证明、驻场人员信息安全等级测评师证书复印件及原件，未经采购方同意，项目组成员不得更改。

## 2) 项目管理保密要求

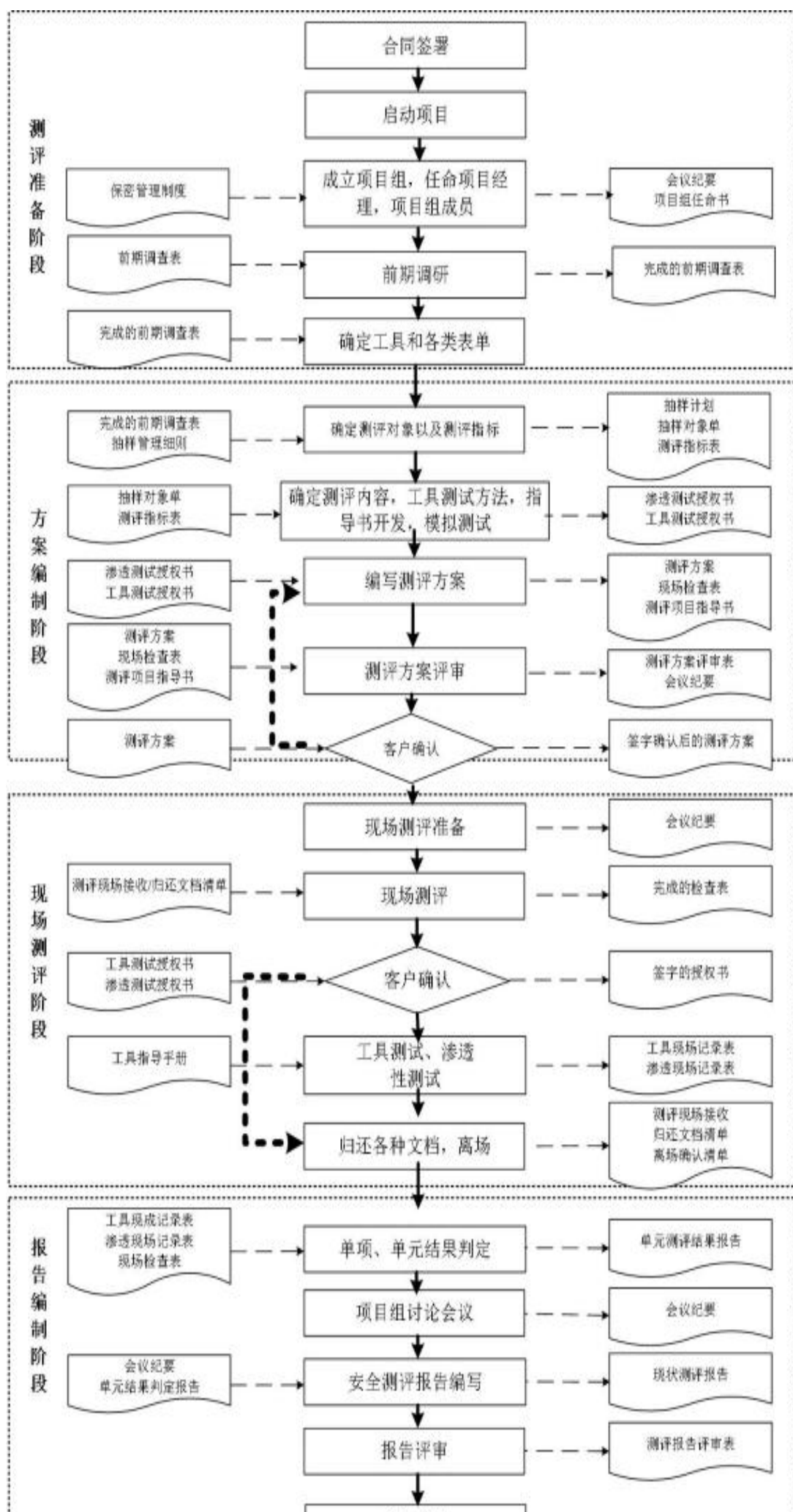
测评机构应与被测评单位签订正式保密协议，并在工作中坚持保密原则，确保应答人及其员工严格规范执行各项保密制度，杜绝任何泄密事件的发生。测评机构需明确将采取的保密措施，对员工的保密管理措施，以及一旦发生泄密事件将采取的措施、需承担的责任，保密责任将长期存在。

## 3) 项目风险控制

测评机构应能够对信息安全等级测评项目过程进行充分的风险考虑，并制定相应的风险规避措施和控制方法。在项目实施过程中，应做好计划与安排，不影响被测评单位正常业务工作的开展。

# 八、实施流程及工作内容要求：

1) 信息安全等级保护测评工作的流程如下图所示，在开展信息安全等级保护测评工作过程中要求严格遵循如下流程：



### ①测评准备活动

本活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测评系统的详细情况，收集被测系统基本资料，形成分析调查结果，准备测评工具，为编制测评方案做好准备。

### ②方案编制活动

本活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测评信息系统相适应的测评对象、测评指标及测评内容等，并根据需要开发测评指导书，形成测评方案。

### ③现场测评活动

本活动是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格执行测评指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

### ④分析与报告编制活动

本活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和行标的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测评系统面临的风险，提出整改意见并配合采购方完成整改，从而给出等级测评结论，形成测评报告文本。

### 2) 测评指标:

#### 三级要求指标:



安全层面	安全控制点	测评指标（2.0）
安全物理环境	物理位置选择	a) 机房和办公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；
	防水防潮	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。
		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	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。
	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。
	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。
		a) 应保证网络设备的业务处理能力满足业务高峰期需要；

安 全 通 信 网 络	网络架构	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。
安 全 区 域	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；
	边界防护	c) 应能够对内部用户非授权联到外部网络的行为进行检测或限制；

边界		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
	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、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
		a) 应在关键网络节点处对恶意代码进行检测和

	恶意代码和垃圾邮件防范	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	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。
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) 应启用登陆失败处理功能，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；
		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、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。
	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	<p>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；</p>
		<p>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。</p>
	数据保密性	<p>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；</p>
		<p>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。</p>
	数据备份和恢复	<p>a) 应提供重要数据的本地数据备份与恢复功能；</p>
		<p>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；</p>
		<p>c) 应提供重要数据处理系统的冗余，保证系统的高可用性。</p>
		<p>a) 应保证鉴别信息所在的存储空间被释放或重</p>



	剩余信息保护	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。
	安全管理	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。
	集中管控	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。
安全管理 制度	安全策略	a) 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；
		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。

	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；
		d) 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。
	评审和修订	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、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。
	人员配备	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；
		b) 应配备专职的安全管理员，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。
	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。

安 全 管 理 人 员	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；
		d) 获得系统访问授权的外部人员签署保密协议，不得进行非授权操作，不得复制和泄露敏感信息。
安	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；

全 建 设 管 理		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。
		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;

	自行软件开发	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。
	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。
	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。
	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) 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。
	服务供应商管理	a) 应确保服务供应商的选择符合国家的有关规定；
		b) 应与选定的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，并对其变更服务进行控制。
	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，物品带进带出和环境安全等方面的管理作出规定；



安 全 运 维 管 理		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。
	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。
	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。
		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，经过审批后才可

	网络和系统安全管理	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；
		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；
		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。
	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) 应建立终止变更并从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。
	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、存储介质和保存期等；
		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

	安全事件处置	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露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) 应确保外包运维供应商的选择符合国家有关规定；
		b) 应与选定的外包运维供应商签订相关的协议，明确约定外包运维的范围、工作内容；
		d) 应保证选择的外包运维供应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) 应在与外包运维供应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、储存要求，对 IT 基础设施中断服务的应急保障要求等。
--	--	---

九、工期

2025 年 10 月 31 日前完工。