网络安全等级保护基本要求 第 1 部分：安全通用要求

一、技术要求：

基本要求		第一级	第二级	第三级	第四级
物理和环境安全	物理位置的选择	/	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	a)； b)；	a)； b)；
	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、鉴别和记录进入的人员	a)	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	a)； b) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员
	防盗窃和防破坏	a) 应将机房设备或主要部件进行固定，并设置明显的不易除去的标记	a) ； b) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。	a) ； b) ； 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	a)； b)； c)；
	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	a)	a) ； 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	a)； b)；
	防火	a) 机房应设置灭火设备	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	a) ； b) ； 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)； b)； c)；

	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	a) ； 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	a) ； b) ； 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。	a)； b)； c)；
	防静电	/	a) 应安装防静电地板并采用必要的接地防静电措施	a) ； b) 应采用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。	a)； b)；
	温湿度控制	a) 机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内	a) 机房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	a)；	a)；
	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	a) ； 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	a) ； b) ； 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) ； b) ； c) ； d) 应提供应急供电设施。
	电磁防护	/	a) 电源线和通信线缆应隔离铺设，避免互相干扰	a) ； b) 应对关键设备实施电磁屏蔽。	a) ； b) 应对关键设备或关键区域实施电磁屏蔽。
网络和通信安全	网络架构	a) 应保证网络设备的业务处理能力满足基本业务需要； b) 应保证接入网络和核心网络的带宽满足基本业务需要。	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) 应保证接入网络和核心网络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网络边界处且没有边界防护措施。	a) ； b) 应保证网络各个部分的带宽满足业务高峰期需要； c) ； d) ； e) 应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。	a) ； c) ； d) ； e) ； f) 应可按照业务服务的重要程度分配带宽，优先保障重要业务。
	通信传输	a) 应采用校验码技术保证通信	a)	a) 应采用校验码技术或加解	a) ；

		过程中数据的完整性		密技术保证通信过程中数据的完整性； b) 应采用加解密技术保证通信过程中敏感信息字段或整个报文的保密性。	b) ； c) 应在通信前基于密码技术对通信的双方进行验证或认证； d) 应基于硬件设备对重要通信过程进行加解密运算和密钥管理。
	边界防护	a) 应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信	a)	a) ； b) 应能够对非授权设备私自联到内部网络的行为进行限制或检查； c) 应能够对内部用户非授权联到外部网络的行为进行限制或检查； d) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。	a) ； b) 应能够对非授权设备私自联到内部网络的行为进行限制或检查，并对其进行有效阻断； c) 应能够对内部用户非授权联到外部网络的行为进行限制或检查，并对其进行有效阻断； d) ； e) 应能够对连接到内部网络的设备进行可信验证，确保接入网络的设备真实可信。
	访问控制	a) 应在网络边界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	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) ； c) ； d) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级	a) ； b) ； c) ； d) ； e) 应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。	a) ； b) ； c) 应不允许数据带通用协议通过。
	入侵防范	/	a) 应在关键网络节点处监视网络攻击行为	a) 应在关键网络节点处检测、防止或限制从外部发起的	a)； b)； c)；

				网络攻击行为； b) 应在关键网络节点处检测和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未知的新型网络攻击的检测和分析； 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	d)；
	恶意代码防范	/		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	a)； b)；
	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。	a) ； b) ； c) ； d) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性； e) 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	a)； b)； c)； d)；
	集中管控	/		a) 应划分出特定的管理区	a)； b)；

				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； 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； 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。	c)； d)； e)； f)；
设备和计算安全	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	a) ； b) ； 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。	a) ； b) ； c) ； d) 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。	a)； b)； c)； d)；
	访问控制	a) 应对登录的用户分配账号和权限； b) 应重命名默认账号或修改默认口令； c) 应及时删除或停用多余的、过期的账号，避免共享账号的存在	a) ； b) ； c) ； 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	a) ； b) ； c) ； d) ； 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；	a) ； b) ； c) ； d) ； e) ； f) ； g) 应对所有主体、客体设置

				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) 应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。	安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。
	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。	a) ； b) ； c) ； d) 应对审计进程进行保护，防止未经授权的中断； e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性	a) ； b) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； c) ； d) ； e) 。
	入侵防范	a) 系统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	a) ； b) ； 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) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞	a) 。 b) ； c) ； d) ； e) 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。	a)； b)； c)； d)； e)；
	恶意代码防范	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)；	a) 应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。	a)；
	资源控制	/	a) 应限制单个用户或进程对	a) ；	a)； b)；

			系统资源的最大使用限度	b) 应提供重要节点设备的硬件冗余，保证系统的可用性； c) 应对重要节点进行监视，包括监视CPU、硬盘、内存等资源的使用情况； d) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。	c)； d)；
应用和数据安全	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，鉴别信息具有复杂度要求并定期更换； b) 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施	a) ； b) ； c) 应强制用户首次登录时修改初始口令； d) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全	a) ； b) ； c) ； d) ； e) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。	a) ； b) ； c) ； d) ； e) ； f) 登录用户执行重要操作时应再次进行身份鉴别。
	访问控制	a) 应提供访问控制功能，对登录的用户分配账号和权限； b) 应重命名应用系统默认账号或修改这些账号的默认口令； c) 应及时删除或停用多余的、过期的账号，避免共享账号的存在	a)； b)； c)；	a) ； b) ； c) ； d) 应授予不同账号为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； 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，客体为文件、数据库表级、记录或字段级； g) 应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。	a) ； b) ； c) ； d) ； e) ； f) ； g) 应对所有主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。
	安全审计	/	a) 应提供安全审计功能，审	a) ；	a) ；

			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	b) ； c) ； d) 应对审计进程进行保护，防止未经授权的中断； e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性	b) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； c) ； d) ； e) 。
	软件容错	a) 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	a) ； b) 在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施	a) ； b) ； c) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	a)； b)； c)；
	资源控制	/	a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； b) 应能够对系统的最大并发会话连接数进行限制； c) 应能够对单个账号的多重并发会话进行限制	a) ； b) ； c) ； d) 应能够对并发进程的每个进程占用的资源分配最大限额。	a)； b)； c)； d)；
	数据完整性	a) 应采用校验码技术保证重要数据在传输过程中的完整性	a)；	a) 应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性； b) 应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性。	a) ； b) ； c) 应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据完整性。
	数据保密性	/	/	a) 应采用加解密技术保证重要数据在传输过程中的保密性； b) 应采用加解密技术保证重	a) ； b) ； c) 应对重要数据传输提供专用通信协议或安全通信协议，

				要数据在存储过程中的保密性。	避免来自基于通用通信协议的攻击破坏数据保密性。
	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	a) ; 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) ; 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热冗余，保证系统的高可用性。	a) ; b) ; c) ; d) 应建立异地灾难备份中心，提供业务应用的实时切换。
	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	a) ; 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。	a) ; b) ;
	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、使用用户个人信息	a) ; b) ;	a) ; b) ;

二、管理要求

基本要求		第一级	第二级	第三级	第四级
安全策略和管理制度	安全策略	/	/	a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。	a) ;
	管理制度	a) 应建立日常管理活动中常用的安全管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度; b) 应对要求管理人员或操作	a) ; b) ; c) 应形成由安全策略、管理制度、操作规程、记录表单等	a) ; b) ; c) ;

			操作规程	构成的全面的信息安全管理制度体系。	
	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	a)； b)；	a)； b)；
	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	a)	a)；
安全管理机构和人员	岗位设置	c) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责	b) 应设立信息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、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责	a) 应成立指导和管理信息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委任或授权； b) ； c) ；	a)； b)； c)；
	人员配备	a) 应配备一定数量的系统管理员、网络管理员、安全管理员等	a)；	a) ； b) 应配备专职安全管理员，不可兼任。	a)； b)； c) 关键事务岗位应配备多人共同管理
	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	a) ； 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	a) ； 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。	a)； b)； c)；

			a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题； b) 应加强与兄弟单位、公安机关、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)； b)； c)；	b)； c)；
	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	a) ； 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。	a)； b)； c)；
	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	a) ； b) 应对被录用人员的身份、背景、专业资格和资质等进行审查	a) ； b) 对被录用人员的身份、背景、专业资格和资质等进行审查，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。	a) ； b) ； c) ； d) 应从内部人员中选拔从事关键岗位的人员。
	人员离岗	a) 应及时终止离岗员工的所有访问权限，取回各种身份证件、	a)；	a) ； b) 应办理严格的调离手续，	a)； b)；