国家档案局办公室关于印发《档案信息系统安全保护基本要求》的通知

档办发〔2016〕1号

各省、自治区、直辖市档案局、馆，各计划单列市档案局、馆：

《档案信息系统安全保护基本要求》已经国家档案局局务会议讨论通过。现印发你们，请参照执行。

国家档案局办公室

2016年1月4日

档案信息系统安全保护基本要求

为指导和规范档案部门进一步加强档案信息系统建设和管理，提高档案信息系统安全保护水平，根据《信息系统安全等级保护基本要求》和《档案信息系统安全等级保护定级工作指南》，结合档案工作实际，国家档案局组织编制了《档案信息系统安全保护基本要求》(以下简称《基本要求》)。

一、适用范围

《基本要求》适用于省级（含计划单列市、副省级市，下同）及以上档案局馆的非涉密档案信息系统安全保护工作。涉密档案信息系统的安全保护，按照国家保密法规和标准进行；涉及密码工作的，按照国家密码管理有关规定进行。地市及以下各级档案局馆可参照《基本要求》的规定进行非涉密档案信息系统的安全保护。

二、编制依据

（一）《信息安全技术　信息系统安全等级保护基本要求》（GB/T 22239-2008）

（二）《信息安全技术　信息系统安全等级保护定级指南》（GB/T 22240-2008）

（三）《信息安全技术　信息系统等级保护安全设计技术要求》（GB/T 25070-2010）

（四）《信息安全技术　信息系统安全等级保护实施指南》（GB/T 25058-2010）

（五）《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

（六）《信息技术　信息安全管理实用规则》（GB/T 19716-2005）

（七）《信息安全技术　信息系统通用安全技术要求》（GB/T 20271-2006）

（八）《电子信息系统机房设计规范》（GB 50174-2008）

（九）《信息安全技术　政府部门信息安全管理基本要求》（GB/T 29245-2012）

（十）《档案信息系统安全等级保护定级工作指南》（档办发〔2013〕5号）

（十一）《数字档案馆建设指南》（档办〔2010〕116号）

三、工作原则

（一）安全引领。建立档案信息系统，要树立“安全第一”的思想，不安全、宁不建，凡已建、必安全。对于准备建设的档案信息系统，要按照同步规划、同步建设、同步运行的原则，建立健全档案信息安全防护体系。对于已建设的档案信息系统，要按照国家有关信息系统安全的要求，查找安全隐患，堵塞风险漏洞，提升安全防护水平，开展定级、测评、整改、检查等信息安全工作。

（二）管理科学。按照计算机信息系统安全等级保护工作谁运行谁管理、谁负责的要求，遵循国家有关信息系统安全保护相关标准规范，结合档案信息系统特点，完善档案信

息系统安全保护的规章制度和操作规程，建立本单位档案信息系统安全管理机制，明确档案信息系统的领导责任和岗位职责。以档案数据为核心，对不同安全级别的档案数据实行区别管理。以预防为主，制定应急预案，定期开展应急演练，妥善应对突发事件。

（三）保障有力。贯彻国家有关文件精神，建立档案信息系统安全管理经费投入机制。配备档案信息系统安全管理人员，定期开展安全培训，为档案信息系统安全保护工作提供有力保障。

四、关于《基本要求》的说明

1.《基本要求》主要以《档案信息系统安全等级保护定级工作指南》中拟定为二级或三级的系统为对象，从“技术”和“管理”两个方面对档案信息系统的安全保护提出了具体要求。

2.《基本要求》中的“等保二级要求”“等保三级要求”中的有关规定均来源于《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）中的规定，“档案行业要求”中的有关规定是根据档案信息系统的特点作出的补充规定。

3.安全保护水平与等保二级保护水平相同的系统，除满足“等保二级要求”中的具体要求之外，还需同时满足“档案行业要求”。安全保护水平与等保三级保护水平相同的系统，除满足“等保三级要求”的具体要求之外，还需同时满足“等保二级要求”，和“档案行业要求”。

五、档案信息系统安全保护的管理要求

（见表 1）

六、档案信息系统安全保护的技术要求

（见表 2）

抄送：各副省级市档案局、馆。

表 1

档案信息系统安全保护的管理要求

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
1安全管理制度	1.1 管理制度	●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； ●应对安全管理活动中重要的管理内容建立安全管理制度； ●应对安全管理人员或操作人员执行的重要管理操作建立操作规程。	●应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。	●安全管理制度、操作规程应涵盖档案信息系统建设、运维的所有工作环节。
	1.2 制定和发布	●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； ●应组织相关人员对制定的安全管理制度进行论证和审定； ●应将安全管理制度以某种方式发布到相关人员手中。	●安全管理制度应具有统一的格式，并进行版本控制； ●安全管理制度应通过正式、有效的方式发布； ●安全管理制度应注明发布范围，并对收发文进行登记。	
	1.3 评审和修订	●应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。	●信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定； ●应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
2安全管理机构	2.1 岗位设置	●应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； ●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。	●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； ●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； ●应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。	●档案馆领导负责对系统权限控制、档案数据处置等重要系统操作活动进行审批。
	2.2人员配备	●应配备一定数量的系统管理员、网络管理员、安全管理员等； ●应配备专职安全管理员，不可兼任； ●关键事务岗位应配备多人共同管理。		
	2.3授权和审批	●应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批； ●应针对关键活动建立审批流程，并由批准人签字确认。	●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； ●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； ●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； ●应记录审批过程并保存审批文档。	●重要审批授权记录应存档备查。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	2.4沟通和合作	●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； ●应加强与兄弟单位、公安机关、电信公司的合作与沟通。	●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，定期或不定期召开协调会议，共同协作处理信息安全问题； ●应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通； ●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； ●应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。	
	2.5审核和检查	●安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	●应由内部人员或上级单位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； ●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； ●应制定安全审核和安全检查制度，规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。	●建立安全检查通报机制，对系统日常安全运行情况进行检查，并将重要安全情况向上级档案部门报告。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
3人员安全管理	3.1人员录用	●应指定或授权专门的部门或人员负责人员录用； ●应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核； ●应与从事关键岗位的人员签署保密协议。	●应签署保密协议； ●应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。	
	3.2人员离岗	●应规范人员离岗过程，及时终止离岗员工的所有访问权限； ●应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； ●应办理严格的调离手续。	●应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。	●关键岗位人员离岗，需将其人员及工作内容信息保留1年以上。
	3.3人员考核	●应定期对各个岗位的人员进行安全技能及安全认知的考核。	●应对关键岗位的人员进行全面、严格的安全审查和技能考核； ●应对考核结果进行记录并保存。	
	3.4安全意识教育和培训	●应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训； ●应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒； ●应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。	●应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒； ●应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训； ●应对安全教育和培训的情况和结果进行记录并归档保存。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	3.5外部人员访问管理	●应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。	●对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。	
4系统建设管理	4.1系统定级	●应明确信息系统的边界和安全保护等级； ●应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由； ●应确保信息系统的定级结果经过相关部门的批准。	●应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。	
	4.2安全方案设计	●应根据系统的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； ●应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案； ●应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案； ●应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	●应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划； ●应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件； ●应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施； ●应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	4.3产品采购和使用	●应确保安全产品采购和使用符合国家的有关规定； ●应确保密码产品采购和使用符合国家密码主管部门的要求； ●应指定或授权专门的部门负责产品的采购。	●应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	
	4.4自行软件开发	●应确保开发环境与实际运行环境物理分开； ●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； ●应确保提供软件设计的相关文档和使用指南，并由专人负责保管。	●应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制； ●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； ●应确保对程序资源库的修改、更新、发布进行授权和批准。	
	4.5外包软件开发	●应根据开发要求检测软件质量； ●应确保提供软件设计的相关文档和使用指南； ●应在软件安装之前检测软件包中可能存在的恶意代码； ●应要求开发单位提供软件源代码，并审查软件中可能存在的后门。	●应要求开发单位提供软件设计的相关文档和使用指南。	
	4.6工程实施	●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； ●应制定详细的工程实施方案，控制工程实施过程。	●应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程； ●应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	4.7测试验收	●应对系统进行安全性测试验收； ●在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告； ●应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	●应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告； ●应对系统测试验收的控制方法和人员行为准则进行书面规定； ●应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。	
	4.8系统交付	●应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； ●应对负责系统运行维护的技术人员进行相应的技能培训； ●应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。	●应对系统交付的控制方法和人员行为准则进行书面规定； ●应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。	
	4.9系统备案		●应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用； ●应将系统等级及相关材料报系统主管部门备案； ●应将系统等级及其他要求的备案材料报相应公安机关备案。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	4.10等级测评		●在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改； ●应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改； ●应选择具有国家相关技术资质和安全资质的测评单位进行等级测评； ●应指定或授权专门的部门或人员负责等级测评的管理。	
	4.11安全服务商选择	●应确保安全服务商的选择符合国家的有关规定； ●应与选定的安全服务商签订与安全相关的协议，明确约定相关责任； ●应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。		

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
5系统运维管理	5.1 环境管理	●应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理； ●应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理； ●应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； ●应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。	●应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理； ●应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。	
	5.2资产管理	●应编制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； ●应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	●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； ●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。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.3介质管理	●应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理； ●应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点； ●应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏； ●应根据所承载数据和软件的重要程度对介质进行分类和标识管理。	●应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定； ●应确保介质存放在安全的环境中，并实行存储环境专人管理； ●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，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点； ●应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁； ●应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同； ●应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。	●存储介质应统一管理，建立采购、使用、检测、销毁的全过程记录； ●存储介质需销毁的，单位应由指定部门统一完成，在送出销毁前需对数据进行清除操作，并将待销毁介质编号登记，以便销毁时查对； ●需长久保存的数据，一般不宜采取加密措施。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.4设备管理	●应对信息系统相关的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； ●应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； ●应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备包括备份和冗余设备）的启动/停止、加电/断电等操作； ●应确保信息处理设备必须经过审批才能带离机房或办公地点。	●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、涉外维修和服务的审批、维修过程的监督控制等。	
	5.5监控管理和安全管理中心		●应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存； ●应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； ●应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.6网络安全管理	●应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； ●应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； ●应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份； ●应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补； ●应对网络设备的配置文件进行定期备份； ●应保证所有与外部系统的连接均得到授权和批准。	●应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； ●应实现设备的最小服务配置，并对配置文件进行定期离线备份； ●应依据安全策略允许或者拒绝便携式和移动式设备的网络接入； ●应定期检查违反规定拨号上网或其他违反网络安全策略的行为。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.7系统安全管理	●应根据业务需求和系统安全分析确定系统的访问控制策略； ●应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补； ●应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装； ●应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定； ●应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作； ●应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	●应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.8恶意代码防范管理	●应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查； ●应指定专人对网络和主机进行恶意代码检测并保存检测记录； ●应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	●应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。	
	5.9密码管理	●应使用符合国家密码管理规定的密码技术和产品。	●应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。	
	5.10变更管理	●应确认系统中要发生的重要变更，并制定相应的变更方案； ●系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。	●应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告； ●应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录； ●应建立中止变更并从失败变更中恢复的文件化程序，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。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.11备份与恢复管理	●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； ●应规定备份信息的备份方式、备份频度、存储介质、保存期等； ●应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。	●应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； ●应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存； ●应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。	●档案数据需进行本地和异地备份。
	5.12安全事件处置	●应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点； ●应制定安全事件报告和处置管理制度，明确安全事件类型，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； ●应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； ●应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。	●应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等； ●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，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存； ●对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.13应急预案管理	●应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； ●应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。	●应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； ●应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期； ●应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。	

表 2

档案信息系统安全保护的技术要求

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
1物理安全	1.1物理位置的选择	●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。	●机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。	●机房建筑抗震不应低于丙类抗震要求； ●机房位置应远离强电磁场、强振动源、强噪声源、粉尘、油烟、易燃易爆等场所和区域。
	1.2物理访问控制	●机房出入口应安排专人值守，控制、鉴别和记录进入的人员； ●需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。	●应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域； ●重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。	●机房等重要区域应配置门禁系统，控制、鉴别和记录进入人员，视频监控记录至少需保存3个月。
	1.3防盗窃和防破坏	●应将主要设备放置在机房内； ●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记； ●应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； ●应对介质分类标识，存储在介质库或档案室中； ●主机房应安装必要的防盗报警设施。	●应利用光、电等技术设置机房防盗报警系统； ●应对机房设置监控报警系统。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	1.4防雷击	●机房建筑应设置避雷装置； ●机房应设置交流电源地线。	●应设置防雷保安器，防止感应雷。	
	1.5防火	●机房应设置灭火设备和火灾自动报警系统。	●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； ●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； ●机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。	
	1.6防水和防潮	●水管安装，不得穿过机房屋顶和活动地板下； ●应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； ●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。	●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。	
	1.7防静电	●关键设备应采用必要的接地防静电措施。	●主要设备应采用必要的接地防静电措施； ●机房应采用防静电地板。	
	1.8温湿度控制	●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。		●开机温度18-28℃，湿度35%-75%；关机温度5-35℃，湿度20%-80%范围内。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	1.9电力供应	●应在机房供电线路上配置稳压器和过电压防护设备； ●应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。	●应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求； ●应设置冗余或并行的电力电缆线路为计算机系统供电； ●应建立备用供电系统。	
	1.10电磁防护	●电源线和通信线缆应隔离铺设，避免互相干扰。	●应采用接地方式防止外界电磁干扰和设备寄生耦合干扰； ●应对关键设备和磁介质实施电磁屏蔽。	
2网络安全	2.1结构安全	●应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； ●应保证接入网络和核心网络的带宽满足业务高峰期需要； ●应绘制与当前运行情况相符的网络拓扑结构图； ●应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。	●应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； ●应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	●局域网与因特网物理隔离； ●涉及重要信息的网段，应进行MAC与IP地址绑定。
	2.2访问控制	●应在网络边界部署访问控制设备，启用访问控制功能； ●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，控制粒度为网段级； ●应按用户和系统之间的允许访问规	●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； ●应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、MTP、POP3等协议命令级的控制；	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
		则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户； ●应限制具有拨号访问权限的用户数量。	●应在会话处于非活跃一定时间或会话结束后终止网络连接； ●应限制网络最大流量数及网络连接数； ●重要网段应采取技术手段防止地址欺骗。	
	2.3安全审计	●应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； ●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。	●应能够根据记录数据进行分析，并生成审计报表； ●应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	
	2.4边界完整性检查	●应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。	●应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； ●应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	
	2.5入侵防范	●应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。	●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。	
	2.6恶意代码防范		●应在网络边界处对恶意代码进行检测和清除； ●应维护恶意代码库的升级和检测系统的更新。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	2.7网络设备防护	●应对登录网络设备的用户进行身份鉴别； ●应对网络设备的管理员登录地址进行限制； ●网络设备用户的标识应唯一； ●身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； ●应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； ●当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	●主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； ●应实现设备特权用户的权限分离。	●网络设备应封闭不需要的端口，关闭不需要的服务； ●建立网络设备运维、管理人员身份数据库，根据职责分配用户名，设置组合或动态密码，分配访问权限。
3主机安全	3.1身份鉴别	●应对登录操作系统和数据库系统的用户进行身份标识和鉴别； ●操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； ●应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； ●当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	●应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
		●应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。		
	3.2访问控制	●应启用访问控制功能，依据安全策略控制用户对资源的访问； ●应实现操作系统和数据库系统特权用户的权限分离； ●应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令； ●应及时删除多余的、过期的账户，避免共享账户的存在。	●应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； ●应对重要信息资源设置敏感标记； ●应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	●禁止单一账户多人使用，禁止使用默认账户及默认口令； ●应根据主机运维部门工作人员职责设置访问权限。
	3.3安全审计	●审计范围应覆盖到服务器上的每个操作系统用户和数据库用户； ●审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； ●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； ●应保护审计记录，避免受到未预期的删除、修改或覆盖等。	●审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； ●应能够根据记录数据进行分析，并生成审计报表； ●应保护审计进程，避免受到未预期的中断。	●系统不支持审计要求的，应以系统运行安全和效率为前提，可采用具备公安机关认证资质的第三方安全审计产品实现审计要求； ●审计记录、报表等应保存1年备查。
	3.4剩余信息保护		●应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
			●应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	
	3.5入侵防范	●操作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，并通过设置升级服务器等方式保持系统补丁及时得到更新。	●应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； ●应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。	
	3.6恶意代码防范	●应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； ●应支持防恶意代码软件的统一管理。	●主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。	
	3.7资源控制	●应通过设定终端接入方式、网络地址范围等条件限制终端登录； ●应根据安全策略设置登录终端的操作超时锁定； ●应限制单个用户对系统资源的最大或最小使用限度。	●应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； ●应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	
4应用安全	4.1身份鉴别	●应提供专用的登录控制模块对登录用户进行身份标识和鉴别； ●应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；	●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。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
		●应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； ●应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。		
	4.2访问控制	●应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； ●访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； ●应由授权主体配置访问控制策略，并严格限制默认账户的访问权限； ●应授予不同账户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。	●应具有对重要信息资源设置敏感标记的功能； ●应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	●应根据用户工作权限分配档案数据资源的处置权限，数据资源输出应审批并限定场所，禁止非授权用户对档案数据资源的添加、删除、更改及复制各类形式副本等操作。
	4.3安全审计	●应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； ●应保证无法删除、修改或覆盖审计记录； ●审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。	●应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	●系统不支持审计要求的，应以系统运行安全和效率为前提，可采用具备公安机关认证资质的第三方安全审计产品实现审计要求； ●审计记录、报表等应保存1年备查。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	4.4剩余信息保护		●应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； ●应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	
	4.5通信完整性	●应采用校验码技术保证通信过程中数据的完整性。	●应采用密码技术保证通信过程中数据的完整性。	
	4.6通信保密性	●在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； ●应对通信过程中的敏感信息字段进行加密。	●在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； ●应对通信过程中的整个报文或会话过程进行加密。	
	4.7抗抵赖		●应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能； ●应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。	●应用系统的操作与管理记录，至少应记录操作时间、操作人员及操作类型、操作内容等信息。
	4.8软件容错	●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数据格式或长度符合系统设定要求； ●在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。	●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。	

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	4.9资源控制	●当应用系统的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； ●应能够对应用系统的最大并发会话连接数进行限制； ●应能够对单个账户的多重并发会话进行限制。	●应能够对一个时间段内可能的并发会话连接数进行限制； ●应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额； ●应能够对系统服务水平降低到预先规定的最小值进行检测和报警； ●应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。	
5数据安全及备份恢复	5.1数据完整性	●应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。	●应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； ●应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	
	5.2数据保密性	●应采用加密或其他保护措施实现鉴别信息的存储保密性。	●应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性； ●应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	●电子档案长期保存数据不宜采取技术加密手段。

一级指标	二级指标	等保二级要求	等保三级要求	档案行业要求
	5.3备份和恢复	●应能够对重要信息进行备份和恢复； ●应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。	●应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放； ●应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地； ●应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障； ●应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。	●应确保存储设备再次分配使用时无任何档案数据，并登记经办人、使用人信息，信息保留1年备查； ●禁止将档案数据存储设备清除数据后分配给非对等权限用户； ●根据需要定期进行增量数据或全数据备份。