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 级要求 | 档案行业要求 |
| · | · | 应 制定信息安全工作的总体方针和安 | 、  · 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。 |
| 1.1 管理  · 制度 | 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 。 |
|  | · | 应指定或授权专门的部门或人员负责 | 安全管理制度应具有统一的格式 ，并 |  |
| 1安全管 理制度 | 1.2制 定 和发布 | 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 ； | 进行版本控制 ；  安全管理制度应通过正式 、有效的方 式发布 ； |
| · | 应将安全管理制度以某种方 式发布到 | 安全管理制度应注明发布范围 ，并对 |
| 相关人员手中 。 | 收发文进行登记 。 |
| ·  1.3评 审  和修订 | · | 信息安全领导小组应负责定期组织相 |  |
| 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。 | 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 二级

指标 指标

等保二级要求 等保二级要求 档案行业要求

·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

·应设立安全主管 、安全管理各个方 面

·档 案馆领导 负 责对系

，并定义各负责人的职责；

的负责人岗位

的负责人岗位 ，并定义各负责人的职责 ； 统权限控 制 、档 案 数据

2.1 岗位 ·应成立指导和管理信息安全工作的委

·应 设立 系统管理 员 、网络管理 员 、安 处置 等 重 要 系 统操作 活 设置 员会或领导小组 ，其最高领导由单位主

全管理 员 等 岗位 ，并定义各个工作岗 位

的职责。

管领导委任或授权 ；

动进行审批 。

·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。

·应 配备一定数量的 系 统管理 员 、网络

2.2人员 管理员 、安全管理员等 ；

2安全管 配备 应配备专职安全管理 员 ，不 可兼任 ； 理机构 ·关键事务岗 位应配备多人共同 管理 。

·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 根据各个部门 和岗位的职责明 确授 应针对系统变 更 、重 要操作 、物理访 权审批部门及批准人 ，对系统投入运行 、 问和系统接入等事项建立审批程序 ，按

2.3授权 网络 系统接入和重 要资源 的访问等关键 照审批程序执行审批过程 ，对重 要活 动 重 要审批授权记 录应 和审批 活动进行审批 ； 建立逐级审批制度 ； 存档备查。

·应 针对关键活 动建立审批流程 ，并由 应定期审查审批事项 ，及时更新需授 批准人签字确认 。 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 。

级 级

指标 指标 等保一级要求 等保 级要求 档案行业要求

·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 应加强 与 供应 商 、业界专家 、专业的

2.4 沟通

和合作

安全公司 、安全组织的合作与 沟通 ·

合作与 沟通 ；

、 ，

·应建立外联单位联 系列表 ，包 括外联

·应加强 与 兄弟单位 、公安机关 、电信

公司的合作与 沟通。

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 。

·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

·建立安全检杏通报机

的一致性、安全管理制度的执行情况等 ·

·安 全 管 理 员 应 负 责定 期 进行 安 全检

制 ，对系统日 常安全运

2.5审核

和检查

应 制定安全检杏表格实施安全检杏

查 ，检查内容包 括系统 日常运行 、系统

汇 总安全检杏数据 ，形成安全检杏报告 ，

漏洞和数据备份等情况 。

并对安全检查结果进行通报 ；

·应制定安全审核和安全检杏制度 ，规 范安全审核和安全检杏工作 ，定期按照 程序进行安全审核和安全检杏活 动。

行情况进行检杏 ，并将 重要安全情况向上级档 案部门报告口

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一级 指标 | 二级 指标 | 等保二级要求 | 等保 级要求 | 档案行业要求 |
| 3人员 安 全管理 | · | 应指定或授权专门的部门或人员负 责 | 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 。 |  |
| 3.1人员 录用 | 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 | 。 |
| ·  3.2人员  · 离岗  · | 应规范人员 离岗过程 ，及时终止离岗 | 应 办理严格的调 离手续 ，关键岗位人 | 关键岗位人员 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 | 员离岗须承诺调 离后的保密义务后方 可 | 需将其人员及工作内容 |
| 以及机构提供的软硬件设备 ； | 离开。 | 信息保留 1年以上 。 |
| 应 办理严格的调 离手续 。 |
| 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  · | · | 应对安全责任和惩戒措施进行书 面规 | ， |
| 应对各类人员进行安全意识教育 、岗 | 定并告知相关人员 ，对违反违背安全策 |
| 位技能培训和相关 安全技术培训，; | 略和规定的人员进行惩戒 ； |
| 应 告知人员相关的安全责任和惩戒措 | 应对定期安全教育和培训进行书 面规 |
| 施 ，并对违反违背安全策略和规定的人 | 定，针对不同 岗位制定不 同的培训计划 |
| 员进行惩戒 ； | 对信息安全基础知识 、岗位操作规程等 |
| 应制定安全教育和培训计划 ，对信息安 | 进行培训 ； |
| 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 级要求 | 档案行业要求 |
|  | 3.5外部 | 应确保在外部人员访问受 控区域前得 | 对外部人员允许访问的 区域、系统 、 |  |
| 人员访 | 到授权或审批 ，批准后由专人全程陪同 | 设备 、信息等内容应进行书 面的规定 ， |
| 问管理 | 或监督 ，并登记备案 。 | 并按照规定执行 。 |
| 4 系统建 | · | 应明确信息系统的边 界和安全保护等级 | ； |  |
| 4.1系统 定级  · | 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 | 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 。 |
| 部门的批准 。 |
| · | · | 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 |
| 应根据系统的安全保护等级选择基本 | 远期的安全建设工作计划 ； |
|  | 安全措施 ，依据风险分析的结果补充和 | 应根据信息系统的等级划分情况 ，统一 |
|  | 调整安全措施 ； | 考虑安全保障体系的总体安全策略 、安全 |
| · | 应以书 面形式描述对系统的安全保护 | 技术框架 、安全管理策略 、总体建设规划 |
| 设管理 |  | 要求 、策略和措施等内容 ，形成 系统的 | 和详细设计方案 ，并形成配套文件 ； |
| 4.2安全 | 安全方案 ； · | 应 组织相关部门和有关安全技术专家 |
| 方案设 | 应对安全方案进行细化 ，形成能指导 | 对总体安全策略 、安全技术框架 、安全 |
| 计 | 安全系统建设 、安全产品 采购和使用 的 | 管理策略 、总体建设规划 、详细设计方 |
|  | 详细设计方案 ； | 案等相关 配套文件的合理性和正确性进 |
| · | 应 组织相关部门和有关 安全技术专家 | 行论证和审定 ，并且经过批准后 ，才 能 |
| 对安全设计方案的合理性和正确 性进行 | 正式实施 ； |
| 论证和审定 ，并且经过批准后 ，才 能正 | 应根据等级测评 、安全评估的结果定 |
| 式实施。 | 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 | 等保二级要求 | 档案行业要求 |
|  | · | 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 |  |
| 4.3产品 |
| 采购和 | 品的候选范围 ，并定期审定和更新候选 |
| 使用  · | 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 。 |  |
| · | 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 。 |  |
| · |
| 4.5外包  软件开 发 |
| · |
| · | · | 应制定详细的工程实施方案控制 实施 |  |
| 应指定或授权专门的部门或人员 负责 | 过程 ，并要求工程实施单位能 正式地执 |
| 4.6工程 | 工程实施过程的管理 ； | 行安全工程过程 ； |
| 实施 | 应制定详细的工程实施方案 ，控制工 | 应制定工程实施方 面的管理制度 ，明 |
| 程实施过程 。 | 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 | 等保二级要求 | 档案行业要求 |
|  | ·  · | · 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 ； |  |
| 4.7测试 | 应对系统测 试验收的控制方法和人员 |
| 验收 | 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 。 |
| · | 应制定系统交付清单 ，并根据交付清 | 应对系统交付的控制 方 法和人员行为 |  |
|  | 单对所交接的设备 、软件和文档等进行 |
| 4.8 系统 交付 | 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，，; | 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 |
| · | 应确保提供系统建设过程中的文档和 | 完成 系统交付工作 。 |
| 指导用 户进行系统运行维护的文档 。 |
| 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 | 等保二级要求 | 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 。 |
| · | 应 确保安全服务商的选择符合国 家的 |  |  |
|  | 有关规定 ； |
| 4.11安 | 应 与 选定的安全服务商 签订与 安全相 |
| 全服务 | 关的协议 ，明确约定相关责任 ； |
| 商选择 | 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 | 等保二级要求 | 档案行业要求 |
| 5系统运 维管理 | · | 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 | 规 |
|  |
| · | 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 ， |
| 5.1 环境 | 范办公环境人 员行为 ，包 括工作人 员调 |
| 管理 | 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 。 |
| · | 应 编制 与 信息 系 统相关 的资产清单 ， | 应根据资产的重 要程度对资产进行标 |  |
|  | 包括资产责任部门 、重 要程度和所处位 | 识管理 ，根据资产的价值选择相应的管 |
| 5.2资产 | 置等 内容； | 理措施 ； |
| 管理 | 应建立资产 安全管理 制度 ，规定信息 | 应对信息分类 与 标识方 法作出 规定 ， |
| 系统资产管理的责任人员 或责任部 门， | 并对信息的使用 、传输和存储等进行规 |
| 并规范资产管理和使用的行为 。 | 范化管理 。 |

，

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一级  指标 | 二级  指标 | 等保二级要求 | 等保 级要求 | 档案行业要求 |
|  | ·  · 5.3介质 管理  · | · | 应建立介质安全管理制度 ，对介质的 | 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 ， 般不宜采取加密措施 。 |
|  | 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 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 ；  应对介质归档和杏询等过程进行记录 ， 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 质归档和杏询等进行登记记录 ，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 要对某单介质实 |
|  | 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 。 |

、

一



．．

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 一级 指标 | 二级 指标 |  | 等保二级要求 | 等保二级要求 | 档案行业要求 |
|  | · | 应对信息 系统相关的各种设备包 括各 | | 应建立配套设施 、软硬件维护方面的 |  |
|  | 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 | |
| 5.4设备 | 等过程进行规范化管理 ； | | 管理制度 ，对其维护进行有效的管理 ， |
| 管理 | 应对终端计算机 、工作 站 、便携机 、 | | 包括明 确 维护人员的责任 、涉外维修和 |
|  | 系 统和网 络等 设备的操作和使用 进行规 | | 服务的审批 、维修过程的监督控制 等 。 |
|  | 范化管理 ，按操作规程实现关键设备包 | |
|  | 括各份和冗余设备 ） 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 。 | |
| 5.5监控 | · | | 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 ； |
| 管理和 | · | | 应 组织相关 人员定期 对监测和报警记 |
| 安全管 |  | | 录进行分析 、评审 ，发现可疑行为 ，形 |
| 理 中心 |  | | 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 | 等保二级要求 | 档案行业要求 |
|  | · | 应 指定人员 对网 络进行管理 ，负 责运 | 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 | 行日 志 、网络监控记 录的 日常维护和报 |
|  | 规定 ； | 警信息分析和处理工作 ； |
| 5.6 网络 | 应 根据厂 家提供的软件升级版本对网 | 应 实现设备的最小服务配置 ，并对配 |
| 安全管 | 络设备进行更 新 ，并在更新前对现有的 | 置文件进行定期 离线备份 ； |
| 理 | 重 要文件进行各份 ； · | 应依据安全策略允许或者拒绝便携 式 |
| · | 应定期 对网 络 系 统进行漏 洞 扫描 ，对 | 和移 动 式设备的 网络接入 ； |
|  | 发 现 的 网 络 系 统 安 全 漏 洞 进行及 时 的 | 应定期检查违反规定拨号上网或其他 |
|  | 修补 ； | 违反网 络安全策略的行为 。 |
| · | 应 对 网 络设 各的 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 。 |

级 级

指标 指标

等保二级要求

等保二级要求 档案行业要求

·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

·应指定专人对系统进行管理 ，划分系

5.7系统 实施系统补丁程序的安装 ；

安全管 应 建立 系统安全管理制度 ，对系统安 理 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 。

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 一 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 | 等保二级要求 | 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 规定备份信息的各份方 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 。 |  |

级 指标

级 指标

等保一级要求

·

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 急预案需要定期审杏和根据

实际情况更新的内容 ，并按照 执行。

等保 级要求

档案行业要求

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 | 等保二级要求 | 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、 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  鉴 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 | 等保二级要求 | 档案行业要求 |
| · | 1.4防雷 | 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。 |  |
| 击 |
| 1.5防火 | · | 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 ； |
| 机房应设置灭火设备和火灾自 动报警 | 机房及相关 的工作房间和辅助 房应 采用 |
|  | 系统。 | 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 | 水管安装 ，不得穿过机房屋顶和活动 | 应安装对水敏感的检测仪表或 元件 ，对 | 机 |
|  | 地板下 ； |
|  | 应采取措施防止雨水通过机房窗 户 、 |
|  | 和防潮 | 屋顶和墙壁渗透 ； | 房进行防水检测和报警 。 |
| · | 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。 |
|  | 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吨 ，湿 度35%-75% ；关 机温度 5-35 吨 ，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 | 应提供短期的备用电力 供应 ，至少满足主 |  |
| 电压防护设备； | 要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 | 应 设置冗余或 并行的电 力 电缆 线路为 计 |
| 足关键设备在 断电 情 况下 的正 常运行 | 算机系统供电 ； |
| 要求 。 · | 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 备寄生祸合干扰 ；  应对关键设备和磁介质实施电磁屏蔽 。 |  |
| 2 网络 | · | 应保证关键网 络设备的 业务处理能力 | 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 E地 址绑定。 |
|  | 具备冗余空间 ，满足业务高峰期需要 ； |
| ·  2.1结构 安全  · | 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 |
| 安全 | 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 。 |
| · | 2.2访问 | 应在网络边界部署访问控制设备 ，启 | 应 能根据会话状 态信息为 数据流提供明 |  |
| 用访问控制功能 ； | 确的允许／拒绝访问的 能力 ，控制 粒度为 端 |
| 应能根据会话状态信息为 数据流提供 | 口级； |
| 控制 | 明确的允许／拒绝访问的能力 ，控制粒度 | 应对进出网络的信息内容进行过滤 ，实现 |
|  | 为 网段级； | 对应用 层HπP 、FTP 、TELNET 、MTP 、 |
| · | 应 按用 户 和 系 统之 间 的允许访 问规 | POP3等协议命令级的控制 ； |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一级  指标 | 二级  指标 | 等保二级要求 | 等保二级要求 | 档案行业要求 |
| · | · | 则 ，决定允许或拒绝用 户对受控系统进 | 应在会话处于非 活 跃一定时间 或会话 结 | 。 |
| 行资源 访问 ，控制粒度为 单个用 户 ； | 束后终止网络连接 ； |
| 应 限 制 具 有 拨 号 访 问权 限 的 用 户 | 应 限制 网络最大流量数及网 络连接数 ； |
| 数 量 。 · | 重要网段应采取技术手段防止地址欺骗 |
| 2.3安全 | 应 对 网络 系 统 中 的 网络设备运行状 | 应能够根据记 录数据进行分析 ，并生成审 |  |
| 况 、网络流量、用 户行为 等进行日 志记 |
| 录； | 计报表 ； |
| 审计 | 审计记录应包括事件的 日期和时间 、 | 应对审计记录进行保护 ，避免受到未预期 |
| 用 户 、事件类型 、事件是否成功及其他 | 的删除、修改或覆盖等 。 |
| 与 审计相关的信息 。 |
| 2.4边界 完整性 检查 | · | 应 能够对非授权设备私 自联到 内部 网络 |  |
| 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。 | 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 、E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、 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 。 | 攻 |
| 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 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 封问不 需 耍的端 口 ，关 阅不 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 | 等保二级要求 | 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。 |
| · | 应启用 访问控制 功能 ，依据安全策略 | 应根据管理用 户的角色分配权限 ，实现管 | 禁 止单一账 户 多人使 |
|  | 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 | 理用 户的权限分离 ，仅授予管理用 户 所需的 | 用 ，禁止使用 默认账户 |
| 3.2访问 | 户的权限分离 ； | 最小权限 ； | 及默认口令 ； |
| 控制 | 应限制默认账户的访问权限 ，重命名系 | 应对重要信息资源设置敏感标记 ； | 应 根据主机运维部 门 |
|  | 统默认账户 ，修改这些账户的默认口令 ； | 应 依据安全策 略严格控制 用 户 对有敏感 | 工作人员 职责设置访问 |
| · | 应及时删 除多余的 、过期的账户 ，避 | 标记重 要信息资源的操作 。 | 权限。 |
| 免共享账户的存在 。 |
| ·  ·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 | 等保二级要求 | 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。 |
| · | · | 应 能够检测 到对重 要服务器进行入侵的 | 、 |
| 操作系统应遵循最小安装的原则 ，仅 | 行为 ，能够记录入侵的源 E、攻击的类型 |
| 3.5入侵 | 安装需要的组件和应用 程序 ，并通过设 | 攻击的目的 、攻击的时间，并在发生严 重入 |
| 防范 | 置升级服务器等 方式保持系统补丁及时 | 侵事件时提供报警 ； |
| 得到更新。 · | 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 | · | 应提供专用的登录控制模块对登录用 | 应 对同 一用 户 采用 两种或 两种以 上组合 |  |
|  | 户进行身份标识和鉴别 ； |
| 4.1身份 | 应提供用 户身 份标识唯一和鉴别信息 |
| 安全 | 鉴别 | 复杂度检查功能 ，保证应用 系统中不存 | 的鉴别技术实现用 户身份鉴别 。 |
| 在重复用 户身 份标识 ，身份鉴别 信息不 |
| 易被冒用 ； |

一级 二级

指标 指标

等保二级要求 等保二级要求 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 。

·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 根据用 户 工作权限

分配档案 数据资源 的处 应具有对 重 要信息资源设置敏感标记的 置权限 ，数 据资源 输出

4.2访问 功能 ； 应 审批并限定场所 ，禁

·应由授权主体配置访问控制策略 ，并

控制 ·应依据安全策 略严格控制 用 户 对有敏感 止 非授权用 户 对档案 数 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。

标记重要信息资源的操作 。 据资源 的添加 、删 除、

更 改及复制各类形式 副 本等操作。

·系 统不支持审计要求

·应提供覆盖到 每个用 户的安全审计功 的 ，应 以系统运行安全 能 ，对应用系统重要安全事件进行审计 ； 和效率 为 前提 ，可 采用

4.3安全 应保证无法删除 、修改或覆盖审计记录 ； 应提供对审计记 录数据进行统计 、查询 、 具备公安机关 认证资质 审计 审计记 录的 内容至少 应 包 括 事件 日 分析及生成审计报表的功能 。 的第 三 方 安全审计产 品

期 、时间 、发起者信息 、类型 、描述和 实现审计要求 ； 结果等 。 ·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 | 等保二级要求 | 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 | 应 采用校验码技术保证通信过程中数 | 应采用 密码 技术保证通信过程 中数据的 |  |
| 完整性 | 据的 完整性 。 | 完整性 。 |
| 4.6通信 | 在通信双方建立连接之前 ，应用 系统 | 在通信双方建立连接之前 ，应用 系统应利 |  |
| 应利用 密码技术进行会话初始化验证 ； | 用 密码技术进行会话初始化验证 ； |
| 保密性 | 应对通信过程中的敏感信息字段进行 | 应对通信过程 中的整个报文或 会话 过程 |
| 加 密。 | 进行加密 。 |
| 4.7抗抵 | · | 应具有在请求的情况下为 数据原发者或 | 应 用 系 统的操作 与 管 |
|  | 接收者提供数据原发证据的功能 ； | 理记录，至少应记录操作 |
| 赖 | · | 应具有在请求的 情况下为 数据原发者或 | 时间 、操作人员及操作类 |
| 接收者提供数据接收证据的功能 。 | 型、操作内容等信息 。 |
| · | 应提供数据有效性检验功能 ，保证通 | 应提供自 动保护功能 ，当故障发生时自 动 | 。 |
|  | 过人机接口 输入或通过通信接口 输入的 |
| 4.8软件 | 数据格式或长度符合系统设定要求 ； |
| 容错 | 在故障发生 时 ，应用 系统应 能够继续 | 保护当前所有状态 ，保证系统能够进行恢复 |
| 提供一部分功能 ，确保能够实施必要的 |
| 措施 。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一级 指标 | 二级 指标 | 等保二级要求 | 等保二级要求 | 档案行业要求 |
|  | · | · | 应 能够对一个时 间段内可 能 的并发会话 |  |
| 当应用 系统的通信双方 中的一方在一 | 连接数进行限制 ； |
|  | 段时间 内未作任何响应 ，另 一方应能够 | 应 能够对一个访问账户或 一个请求进程 |
| 4.9 资源 控制 | 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 ； | 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 ； |
| · | 应能够对单个账户的 多重并发会话进 | 应提供服务优先级设定功能 ，并在安装后 |
| 行限制 。 | 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 | 5.1数据 | · | 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 |
| 应 能够检测到 鉴别信息和重 要业务数 | 复措施 ； |
| 完整性 | 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 务数据在存储过程 中完整性 受 到破 |
| 安全 | 坏 ，并在检测到 完整性错误时采取必要的恢 |
| 及备 | 复措施。 |
| 份恢  复 | 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 | 电子档案 长 期保存 数 据不 宜采取技 术加 密 手 段。 |
| 保 密 性。 |

一级

指标

二级

指标

等保二级要求

等保 一 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 系统的硬件兄余 ，保证 系统的可 用性。

·

· 应提供本地数据各份与 恢复功能 ，完全

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

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 数 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 ；

免 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 。

、