集中化的存储管理是一种非常有效的经济的存储管理解决方案。因为对于磁盘阵列来说，只有一套管理系统，这样就可以极为方便地进行磁盘监控，性能调试。增加或者重新配置磁盘也变得非常简单。最大化的合成集中设备，也使得存储系统的宕机风险降至最低。同时，一套完善的备份方案可以有效地进行数据备份及恢复，确保档案数据的安全。

从以下表来考虑档案数据存储的实现，能够达到较高的冗灾级别。

数据安全	存储	备份	高可用	冗灾
定义	将整个网络的数据集中保存在磁盘阵列	采用专业备份软件将文件、数据库、系统等重要数据全自动、按策略的定时备份到目标存储设备	采用高可用软件将网络服务器、存储设备捆绑，防止网络中任何一台服务器、存储设备的故障造成的网络瘫痪	采用冗灾软件将重要数据“镜像”到另外一个存储设备，防止某一存储设备发生不可抗拒灾难后的数据完整和实时可用
实现方式	NAS/DAS/SAN	专业备份软件	高可用软件	冗灾软件
目标	整和分散存储数据，提高本地数据存储的速度和安全性，提高存储空间利用效率	将重要数据备份后，可以防止系统崩溃、人为误操作、病毒、黑客等对数据的破坏	防止网络中某一台服务器或者光纤交换机、存储设备的故障造成的网络瘫痪	防止发生不可抗拒外力时的数据完整性

好处	提高网络速度、提高数据安全性、方便管理数据和维护	不会因为各种人为原因造成数据丢失	防止因为网络硬件的故障造成网络瘫痪	防止灾难造成的数据丢失和网络瘫痪

从上表可知：

1. 采用存储磁盘阵列实现档案数据的集中存储，提高了数据的传输速度以及数据本地的安全性。

2. 对档案数据的备份可以定时、全自动、按设置好的策略进行，防止人为的误操作、病毒、黑客的破坏。当意外破坏发生后，我们可以按照要求将文件或者数据库数据恢复到我们需要的一个时间点，从而避免各种破坏造成的影响，但它只能将数据恢复到上次备份的时间点，不能做到恢复到任意时刻.

3. 高可用实现后，可以从服务器、光纤交换机、磁盘阵列、连接线缆等各个方面保证整个网络系统时时可用。这是提高网络可用性的关键，即使这些设备发生故障，系统仍然可以使用并没有任何影响，同时能自动报警，及时修复。

4. 冗灾可以保证两个存储设备时时同步，相当于对数据做了一个“镜像”。两个存储设备间的数据完全一致，当某一个存储设备故障后，另外一个存储设备可以自动启用，在保证数据不丢失的情况下维持网络系统的时时可用。但如果出现人为误操作、病毒、黑客的破坏，因为两地的数据是同步的，所以两地的存储同时被破坏，不能恢复到你未被破坏的时间点。

档案数据存储安全应综合考虑以上四个部分，只考虑其中一个和几个不能做到完全意义的档案数据安全，尤其是在备份和冗灾中，各有自身的特点，档案馆可以在统筹考虑资金、安全性等各方面的同时先建设其中几个部分。

4.2.4 查询利用安全保护

档案信息系统查询利用安全保护的主要目标是防止档案信息的扩散，有效防范人员操作的风险、过程的风险等，对这些风险进行预判，做到事前可防范、事中可控制和事后可审计，从而有效保障档案信息的安全，具体地，可以采用以下的策略和技术方式实现：

4.2.4.1 安全策略

档案利用者在进行档案信息的查询利用时，需要按照电子文件与电子档案管理系统的统一安全策略，通过审批流程获得相应的调阅权限。

档案管理系统应根据利用者所使用主机的硬件环境生成机器密钥和借阅人身份密钥对档案进行自动的加密处理，该档案信息将只能由利用者在该主机内正常访问，任何方式的传阅或拷贝在其他终端或工作站都无法访问该档案文件。

同时，档案管理系统对档案信息密级进行分类，当用户需要访问高于某一级别的档案信息时，请求将被重定向到安全终端访问平台，档案信息只能在安全终端访问平台中查看，档案信息不能下载到借阅

主机上，实现数据“终端不留密”要求。

4.2.4.2 输出保护

输出保护主要针对的是档案信息传输和下载的过程。通过输出保护，对电子文件与电子档案管理系统中的档案信息绑定版权信息，有效防止利用过程中通过网络传输的档案信息被窃取，保证档案信息不扩散到不应知悉或获取的范围。

传统档案管理系统中的档案文件在点击下载到终端上查看和操作时，档案信息处于明文状态，由于用户终端或信息网络存在安全和管理的脆弱点，容易造成档案信息外传而导致信息泄密，需要对档案信息进行版权加密保护。应通过版权控制管理技术来保护档案信息，授权给合法用户查阅，保证对档案信息进行不同的操作时，能控制有浏览权限的人是否能复制、打印、摘录、传播，从而保证敏感信息不被泄漏。

1. 加密保护

对电子文件与电子档案管理系统中的档案信息数据进行加密保护，防止信息泄密，主要涉及到数据传输前的加密保护以及在用户终端上的加密保护。可以采用标准的对称算法对文档内容进行加密，使用非对称算法对文档内容的加密密钥进行加密，这样既做到了加密过程的高效，又满足了安全性的要求。加密保护技术实现可以分为以下几个部分：

（1）文档加密：档案信息在传输前可在服务器端结合用户的身

份和密钥进行加密，并写入针对该用户的安全控制信息，只有特定用户才能解密文档，执行权限范围内的操作，即使文档被非法获取，也无法解密。

（2）透明解密：用户读取、打开档案文件时，系统对加密文件进行透明解密，用户无感知，不影响用户正常的与用户体验。

（3）终端保护：通过对终端计算机上部署客户端，进行与档案管理系统相关的档案信息的安全保护，防止由终端操作不当或者病毒入侵等造成的数据安全问题。

对于加密的档案信息的查看过程应无需过多的人工干预，由电子文件与电子档案管理系统根据系统的用户身份密钥和操作权限在后台对加密档案信息进行读写调用：写入磁盘时进行加密，读取和操作时解密成明文供用户操作，用户没有感觉有操作习惯上的变化，文件读取速度上没有明显变慢。要求加密档案信息对象与格式无关，支持通用的办公、图片、视频等文件格式。

2. 水印保护

水印保护实现对档案信息进行版权的显性保护，能够对被打开或打印的文件内容附加水印信息。水印信息中可以添加操作人、部门、操作时间等信息。通过水印保护，即使一些用户进行超出权限范围的拍摄或截屏等操作，也能保障档案信息的版权所有，避免档案信息被非法扩散和传播。水印保护技术实现可以分为以下几个部分：

（1）浏览水印：用户在操作和浏览被保护的档案信息时，在屏幕显示该信息过程中一直附有文件属性的底纹，底纹的内容涵盖用

户、单位、部门、密级等文件属性及警示等信息。底纹的覆盖率超过50%，用于防范随意拍照，通过水印方式警示借阅人员进行拍照等恶意行为。

（2）文件水印：采用水印直接对电子档案进行防护，受保护的电子档案打开时在该文件的内容上自动覆着一层水印信息，水印内容包含组织或部门名称和用户名等相关信息，能够追溯源头，对非法的屏幕截屏等也有一定的防护能力。系统可以设置在用户下载电子档案时即自带水印。

（3）打印水印：由于不少档案利用者在利用档案时想要打印输出档案信息，如果档案信息不加水印就直接输出，有可能被非法利用，因此，在打印档案信息时可以根据需要加入相关的水印信息，水印内容可以包含利用者的唯一身份标识、单位、操作时间等相关信息，既防止通过打印引起的信息泄密，也便于追溯文件使用用户，确定信息外泄源头。

（4）水印信息定制：系统可以根据实际工作需要，定义每份文档要显示的水印信息，以区分不同档案信息的版权保护需要。

4.2.4.3 操作控制

操作控制对应前面的操作过程管控。对用户操作的控制是确保档案信息安全的关键。通过设定安全策略，将管理上的要求嵌入电子文件与电子档案管理系统中，实现对所有档案信息的操作控制，实现档案信息的防泄密和防篡改。

系统应能够控制每个档案信息的操作控制权限，操作控制权限可以定义在一定的期限内、或某个固定终端计算机上，可以进行操作种类等等。

用户应在档案信息安全等级和批准使用方式的约束下对文件进行相应权限的操作，其操作权限严格受到控制，不得超出授权范围以外的操作；禁止非认证的应用程序对档案信息的操作，避免加密信息另保存为非加密信息；用户需要高级别的操作权限时，可以向管理人员申请，经审批通过后系统向用户下放指定档案文件的高级别操作权限；对于使用期限到期的电子档案文件（如文件档案借阅），系统应实现电子档案的回收，达到“覆水能收”的效果。主要采取以下的控制措施：

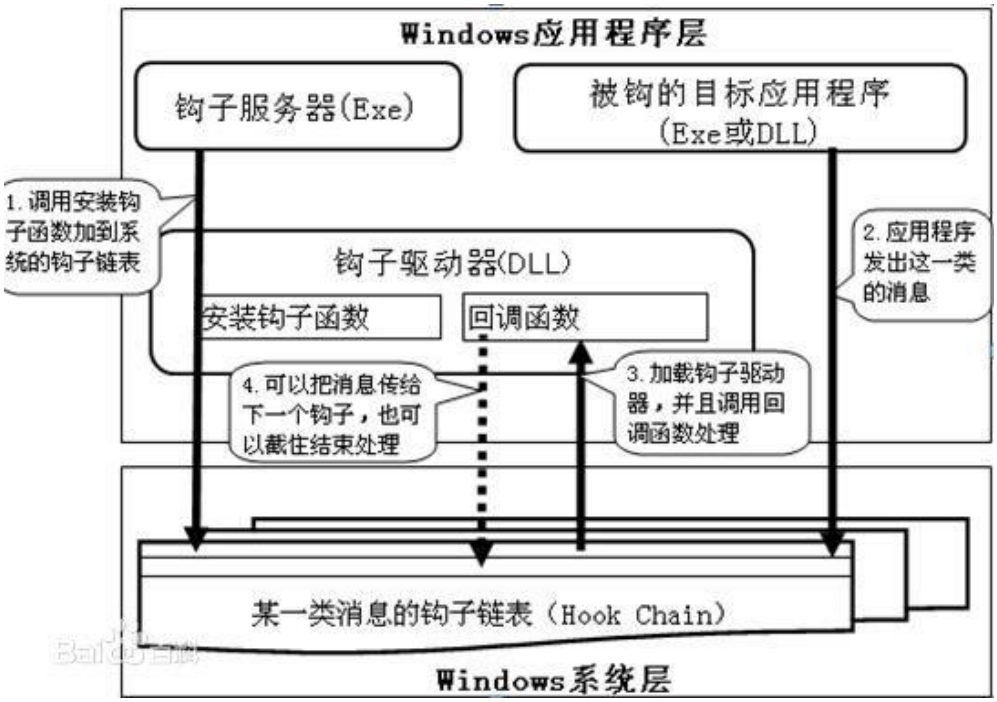
（1）截图控制：通过档案信息安全保护系统的终端读取电子文件头部信息，获取截屏控制策略，如果禁止截屏，终端安全服务会阻止操作系统截屏进程以及第三方截屏工具的操作。

（2）进程控制：终端的安全保护系统可以阻止指定进程对档案信息的访问。如：控制电子邮件、具有网络传输功能的通信软件等对档案信息的访问，有效防止档案信息的非法传播。

（3）操作告警：对正在发生的操作行为进行监控，对非法访问或操作行为进行告警，并通知管理人员。

（4）操作控制：主要通过进程识别技术和 API HOOK 技术来实现。当防护终端识别出正在操作档案信息的进程时，捕获其操作的 API，如截图、保存、打印等，从而改变原有的行为轨迹，实现安全

控制。主要原理如下图：



每一个 Hook 都有一个与之相关联的指针列表，称之为钩子链表，由系统来维护。这个列表的指针指向指定的，应用程序定义的，被 Hook 子程调用的回调函数，也就是该钩子的各个处理子程。当与指定的 Hook 类型关联的消息发生时，系统就把这个消息传递到 Hook 子程。一些 Hook 子程可以只监视消息，或者修改消息，或者停止消息的前进，避免这些消息传递到下一个 Hook 子程或者目的窗口。

4.2.4.4 设备管控

设备管控是指通过对档案信息查询利用中涉及到的设备进行管控来规避设备引起的风险，确保档案信息安全。主要包括：

（1）对每台终端计算机和相关设备进行登记备案，并做好标识，自动发现非法接入的计算机或设备并进行告警；

（2）对移动存储设备如U盘、移动硬盘、手机、平板等进行登记和管控，并做好标识，禁止非法接入终端计算机或存储设备，并进行告警；

（3） 根据工作需要，对计算机上的所有可连通的端口和网络口进行管控，如USB、光驱、Wifi、串口、蓝牙等。如需开通，必须通过管理员的认可，履行相应的审批程序，并进行记录。

（4）对于存储档案信息的存储介质进行加密，即使存储介质丢失，别人也无法解密；导出的档案信息只有在指定人员的计算机上，利用专用的解密工具和KEY才能解密，确保档案信息的安全。

4.2.4.5 主机安全

主机系统安全的目标是确保在查询利用过程中，档案信息在进入、离开或驻留主机时保持可用性、完整性和保密性。它包含一系列关于主机安全的策略和技术手段，通过采用相应的身份认证、访问控制等手段阻止未授权访问，采用防火墙、入侵检测等技术确保主机系统的安全，进行事件日志审核以发现入侵企图，在安全事件发生后通过对事件日志的分析进行审计追踪，确认事件对主机的影响以进行后续处理。

主机系统安全防护包括对档案信息服务器及桌面终端的安全防护。服务器包括各类档案管理应用服务器、网络服务器、WEB服务器、文件与通信服务器等；桌面终端是指作为终端用户工作站的台式机与笔记本计算机。

（1）身份鉴别

应为不同用户分配不同的用户名，确保用户名具有唯一性。对登录主机的用户进行身份标识和鉴别，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，防止身份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身份鉴别技术对管理用户进行身份鉴别。

（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档案信息资源的访问；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；应实现操作系统和数据库系统特权用户的权限分离；应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；应及时删除多余的、过期的帐户，避免共享帐户的存在。

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；

（3）安全审计

应启用安全审计，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；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；应保护审计记录，避免受到未预期的删除、修改或覆盖等。

（4）入侵防范

应能够检测到对重要服务器和终端进行入侵的行为，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。

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。

（5）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；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；并支持防恶意代码的统一管理。

（6）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。

应确保系统内的档案信息文件、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。应限制单

个用户对系统资源的最大或最小使用限度；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。

4.2.5 信息公布安全保护

信息公布中编研开发的情况，类似于之前提到的查询利用过程中安全保护功能的实现，这里我们重点讨论离线利用安全保护的实现。离线利用安全保护的核心是对文件本身操作行为的控制。由于离线利用已经脱离系统管控，因此，对离线调阅的情况应尽量减少，一般只有通过审批才能离线调阅。同时，对离线利用的设备也要进行管控，如指定专用的计算机和存储介质，并对存储介质进行加密，为计算机设置终端防护等，具体地，应实现以下的控制措施：

4.2.5.1 身份认证

在离线利用中，由于档案信息脱离了档案网络环境，需要采用更加严格的用户身份认证方式。因此，可以在基本安全防护的基础上加以强化，对进行操作的用户身份进行认证，除了常用的用户名密码认证以外，可以增加USBKey认证、CA认证、动态口令认证等,如用户必须插入相应的CA并输入正确的密码才能进行操作。

4.2.5.2 操作控制

在离线利用过程中，档案信息的操作控制显得尤为关键。通过设定安全策略，将管理上的要求嵌入档案管理系统中，实现对所有档案信息的操作控制，实现档案信息的防泄密、防扩散和防篡改。

1. 文件操作的控制：文件操作的控制指的是对文件操作本身进行的控制。涉及到以下的控制措施：

（1）打开次数控制：对文件的打开次数进行限制，如限定文件只能打开 3 次。

（2）时效控制：对文件利用的有效期进行控制，如限定文件在 2 天后失效。

（3）拷贝控制：对文件内容的拷贝动作进行监控，限制文件内容的拷贝，防止敏感内容泄密。

（4）保存控制：对文件的保存功能进行控制，防止电子文档被篡改。

（5）另存控制：对文件的另存为功能进行控制，防止泄密。

（6）打印控制：对文件打印操作进行控制，防止通过纸质方式泄密。

（7）硬件绑定：绑定计算机硬件信息，只有指定硬件才能打开文件。

2. 截图控制：终端的安全保护系统读取电子文件头部信息，获取截屏控制策略，如果禁止截屏，终端安全服务会阻止操作系统截屏进程以及第三方截屏工具的操作。

3. 进程控制：终端的安全保护系统可以阻止指定进程对档案信息的访问。如控制电子邮件、具有网络传输功能的通信软件等对档案信息的访问，有效防止对档案信息的非法传播。

4.2.5.3 自动销毁

在档案信息离线利用过程中，可以通过对打开次数和有效期的设置，实现档案信息的自动销毁。

（1）打开次数限制：设置档案信息在离线状态下的最大打开次数，如果达到这个次数，档案信息自动销毁。如设置最大打开次数为3次，档案文件打开三次后，会自动删除。

（2）有效期限制：设置档案信息在离线状态下的有效期，当达到这个有效期，档案信息自动销毁。如设置有效期为3天，3天后，档案信息自动销毁。

4.2.5.4 终端及介质安全

对于离线利用中涉及的终端环境，需要进行严格的安全控制，包括防病毒、设备和移动介质的管控。

（1）定期对终端计算机进行病毒扫描，更新病毒库，并实时监控终端计算机的安全状况。

（2）对每台终端计算机和相关设备进行登记备案，并做好标识，自动发现非法接入的计算机或设备禁止接入，并进行告警；

（3）对移动存储设备如U盘、移动硬盘、手机、平板等进行登记和管控，并做好标识，禁止非法接入，并进行告警；

（4）对存储到终端计算机和移动介质的档案信息进行加密保护，只有通过安全客户端才能够打开离线的档案信息。

4.2.6 对外发布安全保护

对外发布中涉及系统的安全保护，与查询利用的安全保护类似，同时，它又有自己的特点，重点在于防止档案信息在互联网上的非法扩散，保护网站系统的安全，从而有效保障档案信息的安全。具体的，可以采用以下的保护措施：

4.2.6.1 发布审批

所有对外发布的档案信息在发布前都要按照相应的管理权限严格审核批准，设置规范的审批流程，防止未经允许发布档案信息，避免由于管理疏忽而造成档案泄密。发布审批中应包含对发布的具体方式、发布的范围、时限等的审批。

4.2.6.2 操作控制

对所有发布利用的档案信息进行操作控制，功能实现类似于系统调阅中的输出保护和操作控制等部分描述。

4.2.6.3 网站加固

档案信息网站在对外提供服务的同时，可能会受到网络上的各种攻击。网站遭到黑客入侵、网页被篡改或无法访问、停止服务等，不仅仅是档案网站停运的损失，更为重要的是档案信息损失。为保障档案信息的安全，需要对网站系统进行安全加固。

（1）统一安全策略：通过网站系统为档案信息对外发布提供统一

的策略管理和服务，包括用户操作策略、进程策略、文件密级策略、审计跟踪策略等等。功能类似安全管控部分。

（2）主机加固：对网站服务器主机进行加固，包括部署防火墙、入侵检测系统、漏洞扫描系统，安装网页防篡改系统，更新防病毒软件，加固操作系统安全策略等。

（3）网站安全审计：对档案网站进行全面的分析和审计，从用户账号口令、访问控制、系统监测、数据完整、数据加密等多方面进行安全分析和审计。

4.2.6.4 操作审计

从发布审批开始，就要对涉及档案信息的所有操作进行审计。类似基本安全防护中的行为审计，侧重点在于：

（1）审批审计：对发布档案信息的审批流程进行审计，以追溯发布的整个过程和依据。

（2）查询审计：对档案信息的查询操作进行审计，包括查询时间、关键字、用户、IP 地址等关键信息。

（3）下载审计：对档案信息的下载操作进行审计，包括下载时间、用户、IP 地址和权限等关键信息。

（4）审计分析：对所有操作记录进行分析，通过报表和图形进行展现，并进行发现安全风险。

4.2.7 基础安全

除了以上的安全保护功能实现之外，各级国家综合档案馆还应当考虑与档案信息系统相关的基础安全，以保障整个系统的正常运行，确保档案信息利用过程的安全。下面，我们从物理安全和网络安全两个方面来进行探讨。

4.2.7.1 物理安全

物理安全的实现，要通过适当的设备构建，火灾和水灾破坏的防范，适当的通风和空调（HVAC）控制，防盗机制，入侵检测系统和一些安全操作程序。实现这种安全的因素包括物理的、技术的和管理上的控制机制。

1. 物理位置的选择

数据机房和利用场所应选择在交通便利，电力、通信、消防等市政设施齐备，具有防震、防风和防雨等能力的建筑内。

数据机房存储着重要的档案数据，应按照B级及以上电子信息系统机房的标准进行建设；如果机房内的档案数据有涉及国家秘密的，应在机房内设置电磁屏蔽室以保护涉密档案数据，电磁屏蔽室的性能应依据国家相关标准进行。

2. 物理访问控制

（1）数据机房应配置电子门禁系统和视频监控系统，控制、鉴别和记录进出的人员；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；

（2）对档案利用场所应配置视频监控系统，实时记录利用人员的操作和行为；利用场所可根据利用内容和利用对象的不同，划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置过渡区域。

3. 防盗窃和防破坏

（1）将档案信息服务器、存储等主要设备放置在数据机房内；将设备或主要部件进行固定，设置明显的不易除去的标记，并做好相应的台账登记；

（2）应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

（3）对各种存储介质分类标识，存储在介质库或库房中；

（4）对数据机房和利用场所设置监控报警系统，数据机房应利用光、电等技术设置防盗报警系统。

其他防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面的要求可以参照等保要求进行，此处从略。

4.2.7.2 网络安全

档案信息网络安全防护的目的是防范恶意人员通过网络对档案信息系统进行攻击，同时阻止恶意人员对网络设备发动的攻击。在安全事件发生前可以通过集中的日志审计、入侵检测事件分析等手段发现攻击意图，在安全事件发生后可以通过集中的事件审计系统及入侵检测系统进行事件跟踪、事件源定位以发现恶意人员位置或及时制定相应的安全策略，防止事件再次发生。

网络安全防护面向各级国家综合档案馆中的基础支撑网络，以及为各安全域提供网络支撑平台的网络环境设施，网络环境具体包括档案馆网络中提供连接的路由器、交换设备及安全防护体系建设所引入的安全设备。

1. 结构安全

（1）保证档案馆主要网络设备的业务处理能力具备冗余空间，网络系统各个部分的带宽满足业务工作需要；

（2）构建安全可靠的网络拓扑结构，在终端与服务器之间进行路由控制建立安全的访问路径；

（3）根据档案馆内各部门的工作职能、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；

（4）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；

（5）按照档案信息利用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的应用。

2. 访问控制

（1）在档案馆网络边界部署访问控制设备，启用访问控制功能；对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

（2）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；在会话处于非活跃一定时间或会话结束后

终止网络连接；

（3）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；

（4）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对档案信息系统进行资源访问，控制粒度为单个用户；

3. 安全审计

（1）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，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等；

（2）能够根据记录数据进行分析和审计，并生成审计报表；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。

4. 边界完整性检查

（1）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；

（2）能够对档案馆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。

5. 入侵防范

（1）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；

（2）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。

本章通过建立全过程通用的基本安全防护以及档案收集整理、存储传输、查询利用、信息公布、对外发布等各个过程的安全保护重点，兼顾了档案信息利用各个过程安全保护的共性和个性，综合构成了一个有机的安全防护整体。在安全保护功能实现中，针对每个利用过程各自的特点，结合了应用场景，能够主动地对各个环节的风险进行具体的预判，实时、动态地对信息利用的每个操作进行防护并及时做出相应的保护措施。通过有效规范的全过程安全管控，实现了利用过程中档案信息安全保护整体目标。

第五章　保障措施

档案信息利用过程中安全保护是一项系统工程，除了建立安全保护需求方案和具体的实现外，还要有相应的保障措施，才能实现档案信息的真正安全。因此，要有保障信息安全保护工作落到实处的组织机构、规程、策略，以及人才队伍建设的支撑，要用系统性、全局性的思维保障利用过程中档案信息安全保护工作的进行。结合各级国家综合档案馆档案信息安全管理的实际，需要从组织规划、制度规范、日常管理、人才队伍、应急预案等方面加以保障。

5.1 组织规划

5.1.1 组织机构

各级国家综合档案馆应成立相应的部门或者机构负责档案信息安全保护的风险防范、日常管理和指导工作。该组织机构的成立，有利于全方位、系统化地对档案信息的安全进行统一的规划，落实档案行业对于档案信息安全体系建设的要求，对档案馆各工作岗位和业务环节涉及档案信息的安全进行日常的监督和指导，研究档案信息可能面临的风险，提升业务应用系统的安全防护能力，使电子文件与电子档案管理系统达到信息系统安全等级保护以及档案信息系统安全保护基本要求，落实系统管理员和数据管理员的安全责任。

5.1.2 统筹规划

档案信息利用过程中的安全是一项系统工程，不仅仅与信息化技术支持部门有关，更与业务过程中利用到档案信息的各个部门密切相关。必须建立一个完整周密、科学合理的规划，在档案信息利用的各个关键环节中落实安全工作任务和责任，使各部门、各岗位能够互相协作，共同保障档案信息的安全。

在信息安全领域，信息安全的防护强度不取决于安全防护最好的部分，而是取决于最薄弱的环节。信息安全威胁来自方方面面，只要有一个薄弱环节，都可能会导致整个系统无法正常、安全运行。档案管理部门在对档案信息安全进行规划和建设的时候要共同推进各个环节的建设，不能够忽视某一方面。

5.2 制度规范

制度建设是安全的前提和保障，制度的落实保障了标准化工作框架的实施，是解决传统管理中凭借个人主观意志驱动管理的重要手段。建立一套完整的管理制度能够保障各方面工作不会因为各种变化的因素如人员调动、领导变更而改变，而且能够使管理更加简单，需要额外考虑的因素大大减少。一套合理的制度既要求它是完善的、系统的，又要求它能贴合实际，切实可行。

以信息安全为纲，各级国家综合档案馆应本着“防控、补缺、实用”的原则，对已有的信息安全管理制度进行认真清理、修订、完善，完善基础设施安全管理制度、档案数据安全制度、业务系统运行

管理制度等相关制度，明确各部门应履行的职责，确保档案信息的安全管理，将信息安全保护制度落实到信息系统安全规划、建设、测评、运行维护和使用等各个环节，防管并举，才能达到较好的安全效果。

5.2.1 基础设施安全管理制度

各级国家综合档案馆的档案信息主要集中存放在档案馆的数据机房内，机房和档案馆大楼网络环境的安全直接影响电子文件和电子档案这些档案信息的安全。因此，需要建立起档案馆的数据机房和网络环境等基础设施的安全管理制度，如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；对机房内设施设备的安装部署、更改配置、检查维护、故障处理、修理、报废等等均应按规范的程序进行等等。对这些基础设施的管理要落实到人，加强相应的管理。基础设施安全保障问题出现后，要及时地对各种情况记录说明，以便日后的安全分析。

5.2.2 档案数据安全制度

档案数据安全制度的建立，能够规范档案馆档案数据管理，保障档案数据本身的安全，有利于安全可靠地开展利用。档案数据安全制度规定档案数据的收集、生成、移交、接收、维护、存储、备份、利用等各个环节的工作要求、管理责任等等。对档案数据的利用应有严格的规定，包含档案馆内工作需要的利用、来馆查阅档案的利用、通

过网络查阅档案的利用等等。提供利用的管理人员要有较高的安全保密意识，在管理过程中，加强对利用者利用权限的管理等，对安全要求高的档案利用建立严格的审批程序等等，在档案利用制度中都应有体现。依照标准规范收集、管理、保存、利用的档案数据有利于保障数据的安全、可靠。与档案数据安全制度想配套的还有档案数据的标准规范。特别是电子文件与电子档案有一系列的标准规范保障它的真实性、完整性、可读性、安全性，档案数据安全制度的内容应当遵循档案数据标准规范的要求。

5.2.3 业务系统安全管理制度

在电子文件与电子档案管理系统上办理业务必须有一个科学可靠的操作规范遵循，要建立一套业务系统安全管理制度，规定业务系统的安全管理、操作权限分配、操作规范、操作责任、操作监督、数据备份与恢复的管理、软件维护等安全管理机制，可有效降低人为失误，避免一些安全风险。业务系统安全管理制度的建立能保障工作人员在使用档案信息管理系统的过程中按照规定的流程和规范进行操作，不犯安全错误。业务系统运行管理制度与档案信息在利用时的审批制度是相结合的，也能够为电子文件与电子档案管理系统开发时的流程设计提供参考依据。

5.3 日常管理

日常管理工作中最重要的是各司其职，严格落实各项制度。制度

的生命力在于执行，如果执行不到位，再好再完善的制度也会落空。因此，要建立起制度落实的监督机制，制度的执行要有相关记录，便于考核、追踪和分析。

日常管理中有一项重要工作是日常巡检，它是一种主动式的服务，目的在于通过事先的检查，采取必要措施消除故障隐患，保障系统的健康运行。防患于未然是巡检的目的，在日常维护检查和保养中对可能出现的故障或隐患要及时排除，降低系统发生故障的几率，降低档案信息被破坏或泄露的风险。

随着档案信息化建设的发展，各个档案馆都配备了一些网络安全防护产品，为我们掌握档案信息的安全情况提供了很好的监控平台。平时要重视档案信息系统和档案数据的安全，形成定期巡查的制度，根据需要配备巡检人员和工具，必要时可以请有资质的技术公司协助。借助巡检分析系统，及时发现影响档案系统和数据安全的问题，为系统的改善等提供技术依据和计划建议，通过优化、调整参数、配置等方法使系统达到最佳的运行状态，避免档案信息系统崩溃、档案数据损毁。

5.4 人才队伍

5.4.1 人才培养

要实现档案信息安全保护，人是最关键因素，必须培养和造就一批档案信息化建设的人才，特别是精通档案信息安全管理的人才。因此，立足国家综合档案馆信息安全建设和管理需要，制订中长期的档

案信息人才发展规划，出台技术人才培养和技术队伍建设的计划和具体意见，明确人才培养目标和队伍建设要求，科学地指导各地数字档案馆安全体系人才队伍建设，提高各级国家综合档案馆档案信息安全的水平。客观、全面地评价工作绩效，充分体现信息安全管理人员的工作价值，落实奖惩措施，激发工作积极性，是信息安全人才队伍建设发展的重要保证。有计划地为档案工作者提供技术、业务拓展与管理能力提升的培训活动，针对不同岗位制定不同培训计划，为档案工作者的职业生涯发展提供相应的知识更新和技能储备，通过对专业技术人员和档案管理人员的专门培养和深造，使之既掌握各种现代信息技术知识和技能，又了解档案业务，有利于档案业务工作的开展和个人成长。

要加强和鼓励档案工作者对信息安全技术开展研究，如：身份鉴别技术、监控技术、密码技术、冗余技术、文件安全控制技术等，定期邀请信息技术公司人员或图书、情报、计算机等学科专家进行业务交流，提高人才队伍的知识更新频率，以适应档案信息安全形势的不断变化。

5.4.2 人员管理

应定期对档案馆各个岗位的人员进行安全技能及安全认知的考核，应对违背安全策略和规定的人员进行相应教育。落实机房巡查、操作登记等制度，信息安全工作任务落实到责任人。避免没有权限的人员出入相关场所或者进入相关系统或进行违规操作。要害岗位人员

上岗前必须经单位人事部门进行相应审查，技术部门进行业务技能考核，工作经历和工作经验考查等，考查合格者方可上岗。人员离岗应办理调离手续，要害岗位的工作人员承诺其调离后的保密义务，并立即终止其所有访问权限，收回工作中使用的设备，包括工作机、笔记本、移动介质等等。

5.5 应急演练

对于电子文件与电子档案系统以及系统内的档案信息可能遭遇到破坏要有一定的预见性，要将预防这些安全事件发生的具体措施和发生安全事件时降低业务系统和档案数据受损程度的防护措施形成预案，并定期对预案进行演练。

5.5.1 编制预案

应当统一编制档案信息安全相关的各类工作预案，做到既有统一的、纲领性的规范指导，又有针对各类事件而专门制定的应急预案。预案中应根据实际情况，设计工作流程，明确规定动作。

应急预案应规定应急处理的人员组织机构、各岗位的职责、通信联络方式、应急处理的具体措施等等，对可能出现的档案数据损毁、网络病毒木马入侵、黑客攻击、机房核心设备系统严重故障、网络通信中断等等情况分别制定有针对性的措施。

根据应急预案的要求，针对可能发生的几类档案信息破坏情况，配置相应的数据恢复软件及设备，建立一套完善的系统并安排相关人

员负责灾害发生时预案的执行。当网络设备实施发生重大变化或者人员发生变动时，要对应急预案上相应的内容进行调整更新版本。

5.5.2 预案演练

要加强档案信息安全的日常应急演练，突出针对性和操作性。首先，平时就应当重视对档案信息相关系统的监测和预警，定期开展风险分析与隐患排查，并将这些情况有针对性地编入应急预案当中。其次，加强预案演练，可结合国际减灾日、全国消防日及国内的各种灾害纪念日等，定期和不定期地开展应各项预案演练。通过演练能够对各类应急预案的实用性和可操作性、档案数据灾难恢复机制的有效性等进行全面检验，提高工作人员对突发事件的应对效率和对突发情况的处置能力。

演练应选择一些有针对性的场景进行，尽可能模拟真实的环境。演练前要做好相关的准备工作，明确演练目的、人员安排、职责分工和时间计划，并根据演练的需要落实相应的资源。演练中按照应急预案的要求进行演练，通过有关工作检验应急预案的有效性和正确性，并检验各个步骤需要的时间和各岗位互相配合能力等等。演练后要做好总结和评估工作，通过演练评估应急预案实施的成效能否满足需求，对应急预案可能忽略的一些重要需求和问题进行总结，事后的总结和评估能够帮应急预案进一步完善，并及时发现隐患，从而确保档案信息的安全。