档案数字化建设风险及其防控机制

刘　辉

（吉林省梨树县水务稽查大队，吉林　四平　136500）

摘　要：伴随着数字化时代科学技术的发展与深度应用，档案管理正在进行大规模的数字化建设，推动档案管理工作的智能化、科技化、数字化。科学技术和管理理念的革新为档案管理工作方式提供了契机，大大地提升了档案工作效率，拓宽了档案工作的深度和广度。但是科学是具有不确定性和风险性的，任何技术手段都会有其副作用和风险，档案的数字化建设也是如此。在档案工作进行数字化建设的过程中，会出现数字储存空间损耗、网络攻击、系统漏洞等多方面的风险，并且档案管理部门和档案管理人员也会过度依赖电子信息设备，而忽视档案管理专业技能的掌握。为此本文分析档案数字化建设过程中可能会出现的风险状况，并提出了相关的防控机制，期望为我国的档案事业建设提供一些帮助。

关键词：档案工作　数字化建设　风险　防控机制

DOI：10.12319/j.issn.2096-1200.2022.13.13

一、档案数字化建设

（一）档案归档过程的数字化建设

构建数字化档案的第一步是确定要存档的材料。要实现此目的，考虑谁可能使用存档以及他们将需要哪些信息。在进行归档时，需要考虑多个因素，例如记录类型、日期、内容分类、档案访问情况等。我国的党政事业单位档案部门必须考虑他们的目标和他们的服务职能。在选择要数字化的记录时，需要考虑每个档案项目的历史和信息价值，以及档案数量和安全保密等级等因素。对于党政事业单位而言，在决定应将哪些报告、发票、备忘录、会议记录和其他文档数字化时，需要确定时间范围或主题。确定目标和优先事项后，需要了解档案归档的合法权利和责任，也必须考虑知识产权，隐私问题，文化敏感性等。

已经知道存档中将包含哪些类型的材料后，就应该选择可以生成高质量数字文件的最佳数据获取方式，以保留记录的“外观和感觉”。对于纸质文档和照片，首先想到的是图像捕获（文档扫描）。智能数据采集是归档软件最有效和最有用的功能之一。光学字符识别（OCR）可以识别图像和扫描文档中的手写或打印文本，这有助于自动执行数据捕获和分类过程。但可能会受到文档质量的阻碍，可能需要计划对OCR生成的数据进行人工审查，以便验证结果。还需要考虑记录的语言，并确保OCR工具可以读取字符并将其翻译成目标语言。

如果要对大量照片进行数字化归档，则可以使用图像识别工具。该技术可以检测和识别视觉对象，如单位的标志性建筑和标志性符号，对这些摄影记录进行分类。也可以考虑面部识别工具——这个功能强大的人工智能软件可以识别出一张人脸的存在，并将其与已知人脸的数据库进行比较。如果存档将包括视频或音频记录，则需要捕获信息并将其转换为现代计算机可以播放的格式。自动转录工具可用于使这些记录对相关单位的发展和建设更有价值。

创建数字化档案最重要的步骤之一是构建可搜索的索引：如果用户找不到他们正在寻找的信息，档案信息的归档将没有多大用处。可以建设用于纸质存档的索引系统，或者利用这个机会重新思考和修改档案的分类管理策略[1]。调查单位内部的档案使用情况非常有用，这样就可以构建满足其需求的索引。基础数据的一些最基本用途是标识有关文档或记录的以下详细信息：记录和/或馆藏的名称；原始目的或功能；创建的位置和日期；创建、修改、保存或档案原有者的姓名。许多归档软件产品都提供了大量的基础数据字段—如果不需要的某些内容不可用，也可以添加自己的自定义字段。数字存档的主要好处之一是能够将文档相互链接，并使存档用户能够从一个记录无缝移动到另一个记录。这些关系可以基于记录类型、部门、归档人员、主题、日期等。

与任何数字文件一样，档案管理系统需要保护存档免受内部和外部威胁。这包括防止系统故障，以及保护存档免受恶意损坏或删除行为的影响。还需要建立多个备份。归档是一个庞大的、持续的项目，备份可确保为国家未来的发展进行服务。如果数字归档软件不提供强大的备份功能，相关档案管理部门可能还需要投资购买可靠的备份软件。需要通过使用存档软件的访问控制来授予添加、更改和删除条目的权限，从而保护存档的后端。并且需要必须保护前端，尤其是在存档包含敏感材料或资金取决于访问

限制的情况下。

（二）数字化档案基础设施建设

我国的党政机关事业单位在推动数字化档案建设过程当中，十分重视数字化硬件和软件的建设，为数字化档案工作打好了物理条件上的基础。首先是批准档案数字化建设预算，用于购置档案储存硬件和档案管理软件，并且建设硬件设备的机房，用于放置档案数据库、计算机服务器、网络交换机等设备。其次是通过严格且规范的招标活动，购置了专业的档案管理和储存设备，并构建专业的档案管理软件，定期地进行软件的更新和检查，确保档案软件需要适合本单位的职能发挥。

（三）数字化档案人员培养建设

在数字化档案建设过程当中，人力资源是最为重要的环节，只有档案工作人员掌握了一定的数字化档案管理技能，才能推动档案工作的数字化建设与发展。我国现今机关事业单位推动数字化档案建设过程当中，人员培养其主要有以下几种方式：首先是引进相关的档案专业人才，这种人才大多为应届毕业生，他们在高校或研究院所掌握了复合型的档案管理技能，对于数字化档案建设有着一定的了解，并且深刻理解先进的档案数字化管理理念；其次是进行专业的数字化档案工作能力培训，对档案管理部门原有工作人员在档案管理软件操作、硬件维护、档案工作范围扩展等方面进行能力提升[2]。

二、档案数字化建设风险

（一）云计算服务器风险

云计算技术是一种新的IT架构，通过服务级别的划分按需提供计算资源。创新点主要体现在服务模式层面，其商业价值通过资源租赁、应用托管、服务外包等核心运营特征实现。受其结构特点的限制，云计算在给组织和个人带来便利的同时，也不可避免地带来了来自计算机网络环境的安全风险，从而对档案信息资源的安全构成威胁。在计算机学术领域，有学者提出了云计算技术的七大安全风险，分别是特权用户访问风险、合规风险、数据位置的不确定性、共享存储数据风险、数据恢复风险、调查支持（数据跟踪功能）风险和长期发展风险。在云计算的七大安全风险中，长期发展风险和合规风险可以看作是影响云计算技术运行和发展的内外部环境因素，而其他四个风险直接指向数据安全问题。其中，档案数据位置的不确定性风险表明，在档案数据所有权与控制权分离的情况下，数据所有者难以掌握数据的具体物理地址，难以直接监控数据的安全状态。内部数据和机密数据的存储风险不断放大。可以看出，云计算技术所包含的大部分风险都对档案数据安全构成了威胁，这是包含大量数字档案资源的数字档案馆在使用云计算技术时必须重点关注和解决的问题[3]。

（二）数字档案使用风险

与普通的信息管理系统相比，数字档案在信息存储和利用方面具有较强的专业性。数字档案是原始的记录信息，其凭证价值和历史价值是其他类型信息所不具备的。数字档案信息必须真实、未经修改、保存完好、可长期阅读、描述信息完整。这就要求数字档案从内容和载体上为数字档案提供广泛、长期、深层次的安全保障。同时，在信息时代下的数字档案建设中，对信息系统进行安全评估，有利于提前获取数字档案系统的安全风险，进而提出相应的解决方案，这对于提高云环境下数字档案的安全性具有重要意义，但国内在这方面的研究还相对缺乏的，也就说，国内对于云计算攻击、信息攻击等应对可能是不够的。

三、风险防控机制

（一）备份记录体系建设

为保护纸质和电子记录，并确保有价值的备份记录是安全的和可查阅的，建立基本的档案备份记录原则，始终保持档案归档系统和记录存储区域的清晰，当不使用时，没有记录，创建/接收信息和记录后尽快区分保存，记录可以安全持续使用，并尽快删除非记录信息，为所有记录或文件夹指定清晰易懂的名称，以便于电子和纸质记录，可以很容易地归档和检索。销毁副本或方便的副本的记录，一旦你不再需要他们。根据已建立的分类系统或文件计划，将官方记录安全地保存在授权的记录保存系统中，如物理或电子存储库。

（二）管理体系层面

党政事业单位的所有记录，无论是纸质记录还是电子记录，都必须受到保护，避免损坏、丢失、销毁、滥用、未经授权披露、修改和其他风险。无论记录是非机密、机密还是严格保密的，所有人员都必须对记录进行管理，使其免遭丢失、破坏或误用。为了帮助党政事业单位工作人员保护其所有宝贵的信息资产，档案部门可以实施一项全面的信息安全方案。其目标是尽可能安全地保护信息，同时确保各部门的工作人员能够获取信息和记录，以便有效履行职责。有关管理文件和记录的进一步咨询意见，主动和档案专业管理人员联系。有关其他信息安全问题的帮助，可以联系信息和通信技术部门或者第三方服务商的信息安全专业人员。

按照以下步骤来保护电子文件和记录，包括电子邮件：禁止使用计算机硬盘（C：硬盘）存储敏感信息，相反，应将信息的敏感信息存储在正式建立的电子记录保存系统中，或者在没有此类系统的情况下，存储在安全的网络驱动器中。2.定期清理电脑和网络位置，销毁已过期或已过期的记录。3.要认识到，删除电子记录并不等同于销毁它们。与专业的档案信息技术专家合作，确保计算机系统配置确保删除的记录从网络驱动器或其他存储位置永久删除。4.确保计算机系统配置了适当的安全系统、杀毒软件、密码保护和自动超时/锁定功能，以限制只有密码持有者才能访问。5.创建、存储和管理电子记录，以便现在和未来安全、可访问和真实的电子记录。

（三）信息安全层面

首先，建立信息安全防护体系。根据相关文件规定和标准规范要求，建立健全档案信息安全防护体系，开展数字档案信息系统等级保护工作，以提升信息系统整体的安全保护能力，减少安全隐患。加强档案信息资源安全备份工作，可采取增量备份、差异备份或全备份等方式，以及进行异地存储备份，以避免档案信息资源丢失、损毁或操作失误的发生造成的严重后果。

其次，加强档案信息系统日常运行维护。按照国家有关信息系统安全的要求，做好安全隐患排查、风险漏洞检测等工作，提升档案信息系统的安全性。可通过服务外包方式，购买第三方安全服务，开展档案信息系统的日常安全检测、漏洞扫描、风险评估、系统维护等工作，及时消除安全隐患。最后，要做好档案数字化加工的信息安全工作。对数字化加工的设备、网络、数据载体、场所等严加管理，做好档案数字化加工的日常管理和安全保密工作，强化档案实体和数字化成果的安全性、保密性。

（四）技术层面

档案的数字化建设工作是以信息技术为基础而进行的档案工作模式升级。因此在档案数字化建设过程当中，最需要关注的就是计算机技术。

首先，确保应用技术的安全性。任何技术都不可能是完全的安全和稳定，因此再进行档案管理技术的选择时候，要注重相关技术平台未来的改进和稳定能力，改进能力是确保对于技术和系统有足够的升级空间，在计在技术和系统出现漏洞的时候，可以进行有效的填补和修改，而稳定能力是系统进行工作的时候能保持稳定且正常的运转。

其次，档案管理系统和硬件的使用都是需要人为控制的，也就是说在强化安全管理措施流程当中，需要严格把控档案操作人员的安全防范措施。确保相关人员在进入机房或秘密档案储存库时，不携带相关的电子产品，防止部分档案记录的外漏。除安装必要的软件外，禁止安装任何无关软件。加强安装加密软件，以防止私密信息泄露。再次，采取安全加固措施。对档案数字化管理系统的相关服务器进行定期的安全漏洞扫描、病毒检测、风险评估及安全修复工作等。采取专人管理系统登录账户模式，并注意定期更换登录密码。采取内网登录系统的方式，禁止外网接入。关闭系统远程访问功能，避免黑客利用系统漏洞进行登录。最后，做好病毒防控工作。安装杀毒软件、防火墙，并定期进行相关检查。将不常使用的端口保持关闭状态，并利用网络设备的访问控制功能对服务器加以保护。

四、结语

为社会公众服务，满足广大人民群众对档案信息的需求，需要加快推进档案的数字化建设工作。当前，社会及广大人民群众对档案信息的需求与日俱增，人们越来越关注档案信息获取的及时性、方便性，这对档案管理工作提出了新的、更高的要求。档案数字化能最大程度地满足社会对档案信息资源利用的需求，是最大程度地发挥档案服务社会功能的最佳途径之一。但是我们也需要充分地认识到数字化时代的来临，也伴随着一定的风险和挑战，我们需要正视风险，迎接挑战，积极地进行档案数字化工作的内容分析，主动了解风险的来源并提出相应的对策。本文立足于档案数字化的管理工作、数字化建设流程、软硬件建设等因素进行分析，提出了在技术层面，管理体系层面、信息安全、建立备忘录四个方面建立防控机制，为我国的档案数字化建设增添安全的屏障，并助推档案工作的深化扩展。

参考文献

[1]孙冬云.浅析大数据时代的数字化人事档案管理[J].数字通信世界,2019(09).

[2]潘叔霞.云时代中学档案存储及利用研究[J].档案时空,2019(04).

[3]周慧.通信企业档案数字化过程中的保密风险探究[J].通信管理与技术,2021(02):46-48.