

信息时代数字化档案管理方法探究

乔琦

梅里斯达翰尔族区机关事业社会保险服务中心

[摘要]随着我国经济的不断进步,我国已进入信息时代,在此背景下,各行各业都得到了长足的发展。由于目前的档案管理方式技术落后,无法实现与信息时代数据的高速传递和信息资源共享,因此档案管理方式亟需从传统实物管理模式向信息化管理过渡,这便引发出了一个全新的问题,数字文档的安全问题。根据大数码文档的安全,剖析其所存在危险,并建议综合利用加密技术、组织数据库防范管理等措施,实现事前防范、事中管理、事后跟踪的目的,可供国家档案及信息化工程建设和管理参照与借鉴。本文针对数字化档案管理的方法展开分析,并给出相关建议,以期提供参考。

[关键词]数据归档;信息安全防范;密码;数据库

【DOI】10.12252/j.issn.2096-6261.2021.12.211

由于网络、云端计算、虚拟现实、人工智能等崭新科学技术的蓬勃发展,各种档案资料信息也呈现了爆炸性增加,而电子文档的类型也日益多样,依靠人工管理已难满足实际需要,目前档案管理工作人员已开始了从接收纸质文档到电子归档、从文档资料分散使用向公开共享的转变。在提升文档信息检索质量与效率的同时,也一定要严格遵守国家文档安全保密制度、严密保守与管理国家和公司的财务机密,以形成人员安全、物控、技防三位一体的文档安全防范系统,以保护国家与企业的合法权益。

档案信息安全问题是档案事业的发展红线,因此需要进一步提高档案信息系统的安全保护能力。各种关键的资料信息,如果遭到非法修改、伪造和攻击,都会带来不可估量的风险。而档案数据在保存、管理、传递和共享等过程中,也面临着被黑客或木马病毒侵袭、修改的风险,以单纯的信息保密手段很难确保档案数据的安全性,因此必须结合并运用各种信息保密与安全的新技术,构建并加强企业档案管理的预警制度,为企业经济成长、创新发展提供更完整、更方便、更专业、更高效的档案资料管理服务,从而给社会带来更多的效益。

一、档案数字化的必要性

归档的主要价值在于使用,并让归档在经济社会技术进步和个性发展中起到了重要角色。但传统的归档保存管理模式比较简单,由于资讯流通途径窄、信息处理效能较差,且大多是以手工操作方式进行对纸张等载体文档的整理、保存、统计与使用,且工程量很大,无法实现对档案资料数据信息海量的保存、高速的传递、方便的信息检索,以及对数据的资源共享等。随时光流逝,归档实体将会逐步遭受风化、氧化、霉变等多种自然原因环境的影响,并导致在不同程度上出现了老旧、损坏等现象。因此,为了确保馆藏文档的完整、正确和持续利用,应当及时进行实体文档的数字化工作,通过整合建档、编写检索目录、建设各种文档的专题信息库等,变保存为保护,以实现资源科学、高效利用、合理发展的总体目标,功在当代,利在千秋。

目前,文档电子化服务在如下一些领域仍面临着一些明

显缺陷:一是缺少协调计划,重硬轻软、重建轻用,重复建设问题比较突出,各机关文档科室相互之间缺少协调交流,计算机文档运用类软件系统匮乏,导致有路无车、有道难行的情况;二是文档电子化效率不高,对珍贵资料的电子化能力不足,缺少服务性和主动性,不善于找到计算机文档运用的新增长点;三是数字文档资源与现实应用严重脱节,有些电子化资源使用意义不大,缺少具体业务的时效性和针对性,无法满足的真实需要;四是数字化建设激励机制还不够完善,没有政府鼓励,档案工作者的主动性还不够、工作效率不高,管理工作规范化建设尚有待于继续完善;五是信息化工作人才队伍发展还跟不上社会发展要求,随着档案数字化事业的逐步开展,社会迫切需要一批既知文档又懂得信息化工作的复合型专业人才,不过从总体来看,目前参与档案工作的人才中具备高学历的比率仍相当少,且归档人员的素养、技能水平与数字化事业的实际需求尚有相当距离。

二、安全防范技术

1. 数据加密

信息加密是用于文档数据保护中最常用、最普遍的一种方式,它通过专门的数学模型对原始资料进行算法处理后,将核心数据密码以特殊形式传递,比如为无序乱码等,看是否可以传递成功,如果可以成功传递,就可以获得原有数据的密码,进行解密并恢复。信息加密有两种方式进行,主要包括算法和密钥来,算法这种形式,主要是把原来的文字和特殊的组合文字进行组合,这样就可以形成不易理解的乱码,而信息加密与算法不同,是一种对数据信息进行编解码的算法,主要分为两类,一类是对称(私钥)密码,另一类是非对称(公钥)密码。应该选择适合的信息加密方法使用,以确保网络数据的安全传送。这里必须额外补充一点的是,数字签名技术属于公钥加密的一种方法,它附着在原文数据信息之后一同传播,是数据传输方用来证明信息内容真实性的一项数字摘要技术,目的是在网络中取代了以往的手工签章或个人印章,从而具备了防伪、防伪造、可识别等功效。

目前,数字加密技术已相当完善,具有很广阔的发展前

景与应用空间,但仍有其不足之处。首先,是由于秘密文件的脆弱性,在解密时必然需要完整的秘密文件,因此出错也是在所难免的,而一旦秘密文件被修改全部或部分丢失,即使获得了加密也无法复出恢复原诗;其次,是由于加密、破解所带来的巨大运算费用,尤其是一些比较高端、使用性能好的加密算法,其成本也会相应增加。

2. 数字水印

数字水印技术是利用向信息内容上嵌入一种隐蔽的水印标记方法,以证实该信息的真实性和所有权,这种技术不造成被保存信息的外观改变,也不改变该信息内容的真实性,但它很难被未经许可的使用者删除。数字水印技术可以是可见的,也可能是隐藏的、不可见的,而水印技术本身就可以给出真实的识别方法,从而可以为数字打上所有者专属的烙印,以此避免了数据的被歪曲、伪造以及不当传播。数字水印技术可以通过检测水印来证实原始数据内容是否确实完整,从而产生了重要的经济价值。尽管目前的数字水印科技尚无法完全适应实际使用要求,往往只是在出现盗版之后进行追溯而无事先防范,但动态水印科技目前还正处在蓬勃发展当中。对密码以及数字水印技术而言,密钥管理也是一个公认的挑战,但由于密码和水印技术的安全主要取决于密码自身,而并非通过(加密、解密、水印嵌入、水印探查)等方法的安全,所以对保证了密钥管理技术的信息安全者而言,密钥的保护也是十分关键的,涉及密钥的生成、传输、保存、注销、确认等整个流程。所以,对密钥的管理也是当前数码文档安全保护工作的重心。

3. 端口控制策略

电脑的终端很容易受到入侵,必须禁用某些长期不常用的计算机端口才能在网络系统根源上有效防止病毒攻击,具体的做法有限制计算机端口和外设离线状况下正常使用、不可以私自把电脑客户端带出去修理或应用等。而为了防止非法连接和外联,则需要对所有电脑的终端接口和外设实施细粒度的限制。细粒度限制包括了在线和离线两个状态,在线状态是指电脑终端和局域网直接相连的状态,在线状态下合法电脑终端经验证能够直接连通局域网,而非法电脑将面临来自服务器的威胁而无法直接连通局域网;离线状态是指电脑终端与局域网不相连的状况,此时利用终端接口和外设控制策略对电脑的鼠标、按键、无线网卡等个人电子设备实施管理,以防止局域网电脑通过连接其他网络系统或连接互联网而造成的数据信息泄露。

4. 物理隔离

物理隔离技术是使用网络防火墙来保护计算机终端、数据库系统服务器、网络设备等重要硬件实体免受入侵和损坏

的有效技术手段,运用物理位置的阻隔从而保证了数据库系统的安全可靠与稳健性。在物理学上,一个互联网应该被分为内网、外网、屏蔽区三组成部分,内网是受防护的,通常将数据库系统服务器安放在网区内;而外网则是不受网络安全防火墙保障的、不安全的,也就是使用者电脑所在区域;而屏蔽区则是位于国内外网中间的缓冲区,能够让外网使用者借助风火墙来浏览内网服务器设备,也能够在此部署一个开放式的文档与数据信息服务器设备,以供外网用户浏览利用。隔离区比一般的网络安全防火墙增加了一条防护线路,在此外网用户也能够使用分离区内的数据服务器,但没法直接访问到内网的数据库系统,这就在物理上提高了网络系统的安全防范能力。

此外,还必须主要注意一些打印机,因为印刷机设备的运行具有相当的随机性,是安全管理系统中的脆弱环节,最好还是可以做到和外网设施实现物理隔离,甚至关闭与印刷机设备共享以避免关键的档案信息外泄。另外,补丁自行分配也是一项积极的网络安全预防措施,通过过局域网内将操作系统补丁分配至每一位应用终端或自行配置,既能增强对局域网内各种计算机操作系统补丁的管理力量,也可有效防止由于系统漏洞所产生的网络安全问题。

结束语

就目前来看,随着经济的不断发展,社会的不断进步,数字化发展越来越快,与此同时,数字化也处于大变化、大需求的阶段,作为档案保管单位而言,更要顺应时代趋势、未雨绸缪,按照管理一流、服务一流的要求,及时启动并准备档案信息电子化项目、建立数字档案命运共同体,进一步做好对电子文档信息的利用管理和资源共享与合作,进一步建立并健全业务体系,积极推行无纸化办公,积极开展信息在线工作和咨询服务,做到硬件和软件同步,科技和服务并重,深入推动档案管理标准化、馆藏电子化、信息集约化和使用电子化,增强档案数据信息,从而增强社会经济建设的服务功能。

参考文献

- [1]王威威.浅析数字化档案室建设及数字化档案管理技术应用[J].参花(下),2021(12):29-30.
- [2]王玉凤.数字化档案管理创新路径探讨[J].办公室业务,2021(23):111-113.
- [3]冯莹.数字化档案管理系统在工作中的应用[J].中国中小企业,2021(12):169-170.
- [4]赵爽.机关事业单位数字化档案管理工作的实践与探讨[J].内江科技,2021,42(11):10-11.
- [5]潘媛.数字化档案管理面临的制约因素及改进措施[J].兰台内外,2021(27):24-25.