

把握电子档案特性提高档案管理水平体会

郑红

(中国冶金地质总局山东局, 山东 济南 250101)

【摘要】在信息时代,传统纸质版档案已经无法满足档案管理工作需求,电子档案应运而生。做好电子档案管理工作,必须准确把握电子档案特性,优化电子档案传输路径,加强电子档案管理技术建设,从而不断提高电子档案管理水平。

【关键词】电子档案; 特性; 档案管理

电子档案的特性体现在三个方面:第一,存储立体性。第二,资源共享性。第三,管理模式信息化。本文将简单分析电子档案基本特性,并从优化电子档案文件传输路径,严格实施依法治档机制,加强电子档案安全管理网络建设,培养高素质档案管理团队等四个方面分层浅谈如何提高电子档案管理水平。

一、电子档案基本特性

电子档案有三大基本特性:第一,信息存储立体性。电子档案不同于传统纸质版档案,不仅有清晰的文字、图表,而且包括音频档案、视频档案和立体化图像,不少电子档案属于多媒体组合资料,信息存储立体性鲜明。第二,资源共享性。传统纸质版档案虽然有很大的价值作用,却存在时空限制,信息查阅效率低下,经常需要一一翻阅。电子档案不受时间、空间限制,仅需要用计算机输入关键词就能查阅详细的档案信息,具有资源共享性。第三,管理模式信息化。等电子文件归档后,运用计算机系统就能够完成档案资源的全部管理工作,无须像对待纸质版档案那样用大量的时间进行分类整理。其次,纸质版档案存储需要大量的空间,而电子档案所占的存储空间小,而且可以储存大量有价值的信息资源,档案内容更新、传输、查阅速度很快,有效提高了档案资源的应用价值和管理效率。

二、如何提高电子档案管理水平

(一) 优化电子档案文件传输路径

第一,精简。从当代电子档案资源开发利用的视角来看,优化档案在线接收实施路径,需要进一步精简现行档案接收材料。首先要对从未查询利用的材料予以精简化处理。其次,对于纸质材料,应及时采取数字化处理。第二,优化。在档案在线接收工作中,需要进一步优化接收审核流程,在生成电子材料后进行初步审查,然后统一提交给档案管理部门,由档案管理部门进行统一汇总与审核,完成建档工作后,结合实际项目信息内容进行直接匹配共享,这样可以减

少档案的提交。第三,创新。在档案在线接收工作中,应注意对制度、流程和相关技术进行创新,这样方能有效提高工作效率。

必须注意的是,在介绍电子档案的过程中,做好电子档案在线接收前期筹备工作至关重要,首先要做好业务方面的筹备工作,对档案辅导进行提前介入,逐步介入档案在收集、整理领域的指导培训工作。档案的收集开展辅导与培训工作,对于验收通过后未曾及时移交归档,应通过网上公示的方法来实现档案资料传输与共享。其次,要做好常态化培训指导服务工作,构建完善的档案传输制度,以便于提升归档质量与效率。与此同时,要顺应信息时代的发展趋势,做好系统设计工作,完善系统流程环节设计方案,对档案审查接收环节进行全面优化,秉承“前端受理、出证一后台分件、审查”和“分批归档、分批审查”准则,明确“受理、审查、移交(办结)”各环节的办理时限和权责,从而便于及时办理归档和档案审查工作^[1]。

另外,对于电子档案在线接收管理技术领域,应准确把握四项基本要点:第一,做好区块链技术在电子档案接收中的应用研究工作,这样能够确保电子档案生成工作的规范性、档案内容真实性与可追溯性、区块链技术具有一大特征——“记录的不可逆性”,禁止在电子档案生成过程中出行涂改和任意编造问题。第二,做好大数据技术在电子档案接收中的应用研究工作,对电子证照数据的校验匹配展开全面研究,确保电子证照的可验证性,运用大数据技术实现电子证照的可校验与真实性。第三,扎紧制度的牢笼,利用失信联合惩戒机制,对产生电子档案的单位其在电子档案产生、生成和使用过程中的不诚信行为进行联合失信制约,使其一处失信处处受限,净化市场氛围和环境。第四,在技术应用层面,引入目前市场上成熟的电子签名手写板和可信电子签章技术整合集成进入电子档案管理系统中,满足可信电子签名问题。

（二）严格实施依法治档机制

提高电子档案管理水平,加强档案管理信息化建设,确保档案管理质量,理应健全相关法律法规,严格实施依法治档机制。国家已针对当代电子档案管理工作制定了《电子公文归档管理暂行办法》与《电子文件归档与管理规范》,针对电子档案特点和管理工作要求,制定了电子文件形成规范、收集标准、整理方案、归档管理方案、保管利用模式与安全保密管理方案,从而使档案管理工作有据可依,有章可循,进一步提高了电子档案管理规范化、科学化与标准化水平^[2]。

（三）加强电子档案安全管理网络建设

从计算机网络组合来看,电子档案安全管理网络结构层共分为六层:第一,物理安全管理层。第二,网络安全管理层。第三,主机安全管理层。第四,应用安全管理层。第五,数据安全管理层。第六,总系统安全管理层。物理安全管理层来说,其安全防护硬件基础能够保护网络设备和计算机基础设施免于受到自然灾害的损毁,同时,也可以减少人为操作失误对设备的损坏。这一结构层的安全是确保计算机网络信息安全的基础,该层次主要包括基础设施、线路与设备。建设规范的物理安全管理层,能够确保网络 IDC 机房的用电、消防与所处环境符合安全检测标准。

做好存储电子档案的计算机设备网络安全管理层设计工作方能有效解决网络通信安全,确保电子档案传输质量。第一,设置部署访问控制。第二,通过认证加密。第三,设置病毒防御与入侵检测技术。在具体设计工作中,需要严格依据划分区域实施隔离,加强访问控制,禁止非法访问电子档案内容。每个系统均有相应的访问用户,避免安全级别较低的系统因为遇到威胁而影响安全级别较高的系统运行效果,则需要尽量缩小影响面,针对不同安全级别的系统实施相应的划分与隔离。设计完善的主机安全层能够满足整个海量档案文件安全管理需求,在设计该系统的过程中,首先,要做好高性能操作系统的全面安装工作,优化系统安全设置,如果某些端口或者服务不会经常使用,却很容易出现安全问题,就需要将其关闭。其次,要对用户信息、授权和口令进行严格限制,定期更换口令,实现口令组合的复杂化,引导用户不可使用与自身信息相关的组合,也不能应用简单的口令组合。再次,要做好计算机网络系统自动更新程序编辑工作,定期打好补丁。

应用安全管理层属于主机上安装的一种安全应用软件,主要功能是满足电子档案存储计算机设备网络软件所提供的安全应用服务,确保数据信息的安全性,这一结构层组合包括数据库、网页服务、电邮、防火墙和应用网关。应用安全管理层的需要系统会全面记

录使用者的登录信息、退出信息和网页访问信息,同时对这些信息进行统计和分类研究,采取安全警报策略,从而及时发现非法访问,在第一时间通知网络系统安全管理员,也能够发生不安全事件时全面提供查证与举证。其次,当计算机网络出现潜在性未经授权的访问时,该层次会立刻发出安全警示。另外,应用安全管理层能够为检查所得的档案数据信息提供安全可靠的存储方式,维护电子档案信息的完整性,将信息转变为可用资源。

（四）优化电子档案存储安全管理技术

1. 防火墙技术。对于电子档案存储安全管理工作来说,在存储档案资料的计算机设备中,安全防火墙并非实体墙,而是一种有特殊功能的安全访问控制设备,能够在各单位内部网络与 Internet 之间设置一道完整的安全屏障。在大数据时代,数据流在经过网络安全防火墙时会出现三种不同的结果:第一,允许。第二,拒绝。第三,丢弃。防火墙技术的主要功能是根据计算机设备网络系统的安全设置,对未经过授权的数据流实施全面监控、安全限制、针对性选择与屏蔽,这样有助于维护本组织内部网络信息数据的安全。当前网络系统多种设备均配置了防火墙功能,像路由器、交换机和无线基站等设备。与此同时,常用网络操作系统均嵌入了防火墙软件。必须注意的是,部署在出口网络上的硬件防火墙通常无法防御来自内网的攻击,因此,要进行必要的优化,对不安全服务进行科学控制,全方面保护容易受到攻击的服务,加强 IP 地址和协议端口等站点安全访问控制,科学采取集中式安全保护措施,定期实施安全防护扫描,防止 DDOS 和异常包等网络层的攻击。其次,要对站点资源的私有属性予以提升和强化,做好网络层日志的安全管理工作,加强其他安全控制。

2. 入侵检测与防御技术。入侵检测与防御系统技术的英文简称是 IDP 技术,该技术属于一种可以针对违规的网络行为进行自动辨识和采取主动防御措施的系统。安装该系统之后,能够自动做好重要档案数据信息的监控工作,识别数据信息内容,破坏恶意代码与记录侵入。一般情况下,在安全防火墙之前或者之后均可以按照 IDP 系统,该系统不仅能够对入侵的数据流进行及时响应,而且能自动拦截透过防火墙攻击计算机网络的数据流。对于在安装了 IDP 系统的区域网,必须在容易受到入侵攻击的计算机防火墙与服务器附近安装硬件设备。大多数入侵攻击均来自计算机网络出口,而位于防火墙和服务器附近的 IDP 系统可以对大量进出网络的数据流予以及时监控,并自动生成入侵检测报警日志,拦截病毒。

3. 虚拟局域网技术。虚拟局域网技术简称 VLAN, 英文全称是 Virtual Local Area Network, 该技术属于一种虚拟的工作组, 能够对各单位局域网内的设备实施逻辑性划分, 使其转变为多个网段。因而, 可以说 VLAN 技术的核心就是划分网段。在各单位局域网内, VLAN 技术能根据不同的业务与相关安全等级, 按照网段实施安全隔离, 对于网段之间的互访予以严格的控制, 从而有效阻隔网络非法入侵, 防止计算机网络中的档案数据库受到攻击。

4. 虚拟专用网技术。虚拟专用网简称 VPN, 英文全称 Virtual Private Net, 属于私有网络互联技术, 其在公共资源上组合了完整的架构体系, 运用加密技术和专用隧道能够实现数据信息的共享。VPN 技术的重要功能之一是为广大用户提供专用网络, 在专用网中所传输的信息均为私有信息。目前, VPN 技术主要是运用隧道、身份认证技术、加密技术和密钥来维护计算机网络信息的安全, 禁止非法访问电子档案文件, 确保档案信息共享的安全性。

5. 病毒防治与云安全技术。在大数据时代, 随着计算机网络基础建设的优化与完善, 网络覆盖范围也在不断扩展, 网络系统也更容易受到病毒的入侵, 这给电子档案安全管理工作造成的威胁不容小觑。因而, 需要采用先进的病毒防治技术来全面查杀和防治病毒, 避免网络系统受到捆绑软件、下载、压缩性文件、电子邮件、聊天软件和网络共享的负面影响, 在病毒侵扰网络正常运行之前, 病毒防治技术就会及时进行自动阻止。在电子档案网络安全管理工作中, 查杀新病毒的检测方法主要有四种: 第一, 校验和。第二, 特征代码。第三, 行为检测。第四, 软件模拟法。目前, 云安全技术能够对网络病毒库的更新不及时产生的负面影响予以有效解决。云安全技术可以结合大量客户端对应用计算机网络服务软件的异常检测结果, 将所获取的恶意代码与木马病毒信息传输到云端, 然后, 将处理结果发送给所有用户端。该技术能够满足用户量越多越安全的需求, 可以覆盖到所有局域网, 一旦发现网络异常就会立即得到消息, 并及时将病毒库的单机查杀转换成网络查杀, 全面预防新病毒入侵问题。

6. 系统安全加固技术。计算机网络系统安全加固技术能够有效提升计算机网络操作系统与各种应用服务软件质量, 做好相关优化配置工作, 进一步提高计算机网络安全等级, 增强网络防御能力, 为做好电子档案网络安全管理工作提供完善的保障。从整体上看, 网络系统安全加固技术有两项应用要点: 第一, 对补丁进行升级, 实现服务最小化。第二, 加强安全认证管理工作, 严格设置每一位用户的访问权限, 同时对

子目录的访问权限进行合理划分。

7. 漏洞扫描与评估技术。漏洞扫描和评估技术属于一种针对网络信息安全所处风险实施客观评估的技术, 该技术可以在事先识别网络受到攻击入侵性访问的可能性, 及时发出异常警告, 输出产生的后果。同时, 计算机网络漏洞扫描和评估技术能够对排查对象的资源进行协助辨别, 准确判断网络资源是否受到攻击, 明确当前的网络弱点, 准确评估网络信息安全风险。

8. 数据容灾备份技术。在电子档案网络安全管理工作中, 数据容灾备份技术属于不可或缺的重要技术, 该技术以实现网络化与虚拟化为发展方向, 能够采取科学合理的措施, 结合电子档案内容设置好备份, 做好档案信息安全存储工作。在发生各种事故时, 数据容灾备份技术能够将备份档案数据的丢失量控制到最低, 并采取应急响应的处理措施, 使网络系统及时恢复运行, 避免出现因为意外丢失数据而导致电子档案内容不全。

(五) 培养高素质档案管理队伍

档案管理部门应不断提高档案管理人员的专业能力, 要求档案管理人员不断提升个人素养, 加强自身在档案专业管理知识、文化基础知识、计算机水平、网络能力、外语水平等方能的能力, 恪守职业道德。与此同时, 档案管理部门应注意引导全体档案管理人员正确认知电子档案管理目标, 熟练运用智能化技术做好电子档案管理工作, 在保密的基础上合理开发档案资源, 以便于发挥档案的应用价值, 运用档案资源促进本单位各项管理工作的发展^[4]。

结语:

综上所述, 全面提高电子档案管理水平, 确保电子档案接收工作的顺利实施, 必须重视优化电子档案传输路径。同时, 要发挥《电子公文归档管理暂行办法》与《电子文件归档与管理规范》的作用, 坚持依法治档。在信息时代, 应着重加强电子档案网络管理安全建设, 优化档案安全管理技术。另外, 档案管理部门应做好档案管理人员的职业素养与技能培训工作。

参考文献:

- [1] 林明艳. 档案管理基础工作在现代档案管理中的重要性 [J]. 现代国企研究, 2018(8):79.
- [2] 李进鹏. 提高档案管理科学化水平的路径选择 [J]. 行政事业资产与财务, 2020(14):123-124.
- [3] 张思文, 胡建. 浅谈档案库房安全管理再改造 [J]. 治淮, 2018(2):32-33.
- [4] 郑雪梅. 档案库房管理中现代化技术的应用研究 [J]. 江西建材, 2019(4):297+300.