关于电子档案信息安全保障工作的思考

王海啸

（河北省承德市滦平县社会保险事业管理局　河北　承德　068250）

[摘　要]档案数据与一般的信息内容不同，它记录了党政管理主题活动的时间和全过程。很大一部分档案与国家机密和国防安全有关，包括国家政治、经济发展、高科技、国防、文化艺术等领域的内容，具有较强的安全性和应用约束。非法使用此类信息内容将影响国防安全，危害群众权益，严重危害社会稳定。档案信息内容独特的内在性质，决定了其在数字自然环境中存储和传输的稳定性要高于其他信息内容。怎样提高档案数据和变更的安全系数是档案存储信息时代必须直接面对的难题。

[关键词]档案信息；信息公示；网络信息安全

【DOI】10.12252/j.issn.2096-6261.2021.06.1407

一、档案信息内容安全范围

档案数据的安全性包括三大类：（1）安全性和保密性：使不合法授权的人不能使用它；（2）真实有效：能够明确档案数据的合理合法来源；（3）一致性：确保档案数据未被故意或无意伪造。根据梳理出的稳定性范围，本次相关通信和数据传输过程中的各类安全要求可进一步分类为：安全要求；真实有效的要求；一致性要求。为了更好地满足这三个安全要求，必须针对档案的管理和控制设计更加细致的保护体系。

电子文件和档案的管理和控制的整个过程完全是通过使用电子计算机来实现的。所以，要在互联网的各个节点上进行文献信息的免费归档和档案资料资源共享，完成档案资料的信息公示，就需要创建互联网系统软件。众所周知，在网络空间中文件数据的传输和存储过程中，每个过程都可能出现网络安全问题，极易受到黑客入侵，导致文件数据严重泄漏、信息被盗、更改或删除，反过来又将档案数据的发布和营销限制在一定的水平。所以，在档案数据保护体系中，应制定预防方案和应急方案，以确保档案信息公开的安全系数。

二、档案信息的安全设计方案

（一）员工安全

文件数据网络信息安全系统软件，无论设计方案多么严谨，如果没有严格的人员控制，无论使用多么复杂的加密算法，都只是流于形式。因此，文件信息内容操作的过程中最大可能存在的安全隐患是人为因素的泄漏。所以，在没有公开档案信息时，要杜绝一切有意或无意的人为因素疏忽。对文教机构团队成员进行培训后，积极宣传网络信息安全的必要性，降低引发的概率。而且，在应用档案信息内容之前，大家严格遵守，在进入归档数据仓库之前，要首先确认用户的真实身份。另外，由于档案部门的所有成员都会了解档案的不同层次，人员变动，包括人员变动，辞职、辞退等，都会导致信息内容的丢失，为防止档案信息内容意外泄漏，需要制定人员变动管控和管理权限有效期的管理办法。当所有工作人员接触到计算机上的文件信息内容时，首先要获得该区域计算机的所有权，并对用户的管理权限实施监督。根据不同职位的权限，授予一般应用程序、特殊用户或管理人员管理权限。以稳定用户账号命名的逻辑，基本上可以在很多方面识别人力。如果有侵入意图，应用程序没有管理权限的代码，可以立即删除。严格管理同事使用不易被他人猜到或看到应用的驾驶登录密码、强制登录密码的长度和组成复杂度（如强制英文、数据掺杂），降低被“故意”猜到的概率；在电脑上离开座位时，运行屏幕保护程序的账户密码等。

（二）实际操作安全

对员工开展网络信息安全文化教育，可以确保现行网络信息安全。除了宣传网络信息安全意识外，还应重点关注档案信息内容运行过程的安全，包括个人电脑防污染对策，以及材料备份数据的意识；防止文件信息泄漏链接不经意间携带计算机病毒传播出去，导致用户破坏或伪造文件信息的内容。文件数据单位除在文件网络服务器上安装杀毒工具外，还应在电子邮件服务器上安装电子邮件计算机杀毒软件，营造基本的杀毒安全自然环境。今天的计算机病毒是无所不能的。所以要养成备份关键资料数据的习惯，关键文件数据备份到网络服务器上，备份到光盘或硬盘上，减少不成功的概率恢复。关键的是要树立异地备份数据的意识，在备份数据工作中依法依规。在这里，制定网络信息安全保护预案和应急方案，并定期对确定的网络信息安全相关条款进行调整和反省，确保网络信息安全预案的可行性分析，使安全通报程序过程出乎意料。成为档案资料单位成员所了解的基本常识，推动档案安全工作的实际运行具有实践依据。

（三）档案信息安全

档案单位可携带的已公示档案信息内容主要以电子邮件和网页浏览的形式进行操作。为了更好地保证已发布的个人文件信息内容的应用安全，请使用杀毒软件和邮件扫描软件进行消毒；采用网页方式发送时，采用内容过滤装置和拦截网页浏览系统软件，保证所张贴材料的安全，防止发布后可能造成的危害。

在这个阶段，整个文档以图像为主。图像扫描仪的整个过程很可能会遇到人为因素的安全风险或材料打字基本相同的问题。所以，要非常注意获取原始卷的整个过程。扫描仪前后的原件总数应尽可能保持一致，原件不得损坏、故意删除或被盗。

为更好地避免档案信息内容被窃取，保证档案单位发布的个人档案信息内容的唯一性和可信性，需要先对档案进行加密，同时配合相互之间进行声音存储。采取控制措施，防止管理权限不足的人员获取材料。众所周知，存储加密算法再完美，也无法防止系统软件人员误操作。为更好地防止使用中人为因素的疏忽和纠纷，需要在全套文件数据操作过程中构建完整的系统软件文件，以方便日后跟踪研究，使文件数据的实际操作可以称为安全。另外，还需要制定相关法律法规作为依据。

档案资料是中国宝贵的历史文化财富，为中国政治、经济发展、文化艺术、国防建设提供了不可替代的数据支撑点。档案安全是档案信息公开的前提。建立档案信息公开的可行性，需要有良好的网络安全自然环境。众所周知，基于计算机和网络通信的方式进行档案信息公开，很难保证绝对的安全保护。因此，对于一些秘密档案，建议不要立即在线传输。特别要禁止在互联网上发布涉及国家秘密的档案资料。此外，要树立文件信息网络信息安全从我做起的意识。档案和网络信息的安全不是仅仅由某些人或某些产品来保证的。与档案管理工作相关的技术人员必须在安全和信息保密方面达成共识，才能在网络技术的应用中维护档案安全。

参考文献

[1]陈铁飞.关于电子档案信息安全保障工作的思考[J].关爱明天，2015（3）：7-7.