电子档案证据效力维护规范

Preservation standard for evidential validity of electronic archives

(征求意见稿)

前 言

本文件按GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由国家档案局提出并归口。

本文件起草单位：国家档案局技术部、苏州大学社会学院、苏州苏大苏航档案数据保全有限公司。

本文件主要起草人：XXX、XXX。

电子档案证据效力维护规范

# 1 范围

本标准规定了维护电子档案证据效力的一般要求与方法，包括电子档案证据效力维护的总体性要求、具体工作要求和电子档案存证技术要求等。

本标准适用于机关、团体、企事业单位和其他组织的档案室、档案馆在电子文件归档和电子档案管理过程中对档案证据效力的维护，其他活动中形成的各类文件数据等可参照本标准实施。

# 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 29194—2012 电子文件管理系统通用功能要求

GB/T 18894—2016 电子文件归档与电子档案管理规范

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 39784—2021 电子档案管理系统通用功能要求

DA/T 56—2014 档案信息系统运行维护规范

DA/T 70—2018 文书类电子档案检测一般要求

SF/T 0076—2020 电子数据存证技术规范

# 3 术语和定义

GB/T 18894—2016、GB/T 22239—2019界定的以及下列术语和定义适用于本文件。

3.1

电子档案证据效力 evidential validity of electronic archive

电子档案作为法律证据所具有的对特定事项的证明力。

3.2

电子档案存证 verification of electronic archive

通过电子签名、加盖时间戳、提取并固化电子档案完整性校验值、上传区块链保存等法律认可的技术手段对电子档案原始性予以固定、保存和验证的操作。

3.3

电子档案存证平台 electronic archive verification platform

由电子档案保管机构或电子数据存证服务提供方构建的用于实现电子档案存证功能的软硬件设施及系统。

[来源：SF/T 0076—2020，3.4，有修改]

3.4

电子档案数据保全系统 electronic archive preserve and verify system

提供电子档案证据效力维护，具备电子档案存证、存储数据监测、错误修复、保管过程追溯等功能的信息系统。

3.5

可信时间标识 trusted timestamp

从国家可信时间源获取，唯一地标识某一刻时间的字符序列。

[来源：SF/T 0076—2020，3.5，有修改]

3.6

时间可信 time credible

系统时钟及操作过程中生成的时间标识均来自国家可信时间源的授时，并可通过生成时间戳等方式记录和验证其准确性。

3.7

完整性校验值 integrity check value

对电子数据采用完整性校验算法计算得出的字符串，用于固定和验证电子数据的原始性。

[注：本标准所述完整性校验值以SM系列国家商用密码算法得出。]

# 4 电子档案证据效力维护的总体要求

4.1 应遵循“来源可靠、程序规范、要素合规”的原则，遵守电子文件归档与电子档案管理的法规和标准，依照电子数据证据保护的法定程序和要求切实维护电子档案数据的真实性、完整性、可用性和安全性。

4.2 应建立安全可靠的电子档案管理体系，保证电子档案始终在受控、可信赖环境下生成、归档、保管和利用，确保电子档案的管理过程连续、规范，操作内容和操作时间明确，实施主体身份确定、保管环境和管理过程记录完备并可追溯、内容原始性可验证。

4.3 应采取必要技术手段，对电子档案实施原始性固定、存储状态监测、技术环境跟踪，并通过可信网络或离线设备执行电子档案的存证与验证。

# 5 电子档案证据效力维护的具体要求

# 5.1 电子文件归档

5.1.1 电子文件应在符合规范要求的业务系统中生成、流转和使用。

5.1.2 电子文件生成、流转和使用中应同步形成完整的日志信息，记录关键节点的可信时间标识、存储路径等信息，并确保与电子文件间的关联。

5.1.3 应完整归档电子文件及其元数据。元数据采集遵照GB/T 33480—2016、GB/T 26163.2—2010、DA/T 46—2009、DA/T 54—2014、DA/T 63—2017的规定。

5.1.4 电子文件归档宜生成信息包（EEP），以维护电子文件及其元数据的稳定关联。信息包的内容及其封装结构应遵循DA/T 48—2009的规定。

5.1.5 电子文件业务系统不具备生成信息包功能，或者电子文件在系统外单独形成时，除完整归档电子文件及其元数据外，还应归档以下要件之一：

a）责任主体对归档电子文件及其元数据所做的电子签名；

b）责任主体对归档电子文件及其元数据加盖的时间戳；

c）责任主体对归档电子文件及其元数据所做并通过存证平台存证的完整性校验值。

5.1.6 业务系统内电子文件的归档应在不脱离系统监控的前提下，基于安全可靠的信息网络导入电子文件管理系统或电子档案管理系统。传输过程中应采用校验技术来确保数据传输的安全性。无法借助安全网络在线提交或不经业务系统形成的电子文件，可采用离线递交介质的方式归档，提交前后应实施完整性校验。

5.1.7 归档时接收方应确认归档主体身份的真实性和合法性，线上通过CA认证或其他可靠身份认证手段确认，线下通过身份证件或签章信息确认。

5.1.8 归档时交接双方应验证归档数据的真实性和完整性，验证手段包括：

a）验证信息包中的电子签名和锁定签名，确认其正确无误；

b）计算归档数据的完整性校验值，与原始校验值比对，确认两者一致；

c）采取法律认可的其他数据完整性校验方法。

5.1.9 归档时接收方应检查归档文件制作工具和生成系统的合法性，排除非法软件或系统制作的文件，并对文件实施病毒查杀，确保归档文件的可靠性。

5.1.10 归档环节应以纸质或电子方式制作归档登记表，记录归档电子文件内容、数量、来源、文件制作软件、归档方式，归档时间、归档责任主体、归档数据的真实性、完整性、可靠性检测方法及结果。归档登记表格式参照GB/T 18894—2016附录A规定，宜增加完整性校验值和归档存证信息等记录项。归档登记表必须由交接双方以电子或传统方式签章生效，并归档保存。电子方式的归档登记表，宜同时存证。

# 5.2 电子档案存储和保管

5.2.1 电子档案应在安全、稳定、可靠的软硬件及网络环境中存储、保管，其管理系统应符合GB/T 29194—2012、GB/T 39784—2021第4.4条的要求，系统安全等级保护遵循GB/T 22239—2019第8.1条的规定，运行维护符合DA/T 56—2014的要求。

5.2.2 应按照GB/T 8567规定的内容保存系统开发、测试过程中形成的技术文档，特别是系统设计文件和系统评测报告，并保存系统部署方案及其配置信息。

5.2.3 电子档案管理系统的时间及生成的可信时间标识应从国家可信时间源进行授时和守时。

5.2.4 应实时记录电子档案存储、保管的关键业务过程，形成并保存完备的系统操作日志。

5.2.5 应规范实施运维管理，确保系统、网络、设备的正常运行，形成并保存运维记录。

5.2.6 应严格实施系统的安全检查和审计跟踪，形成并保存系统安全管理和审计跟踪记录。

5.2.7 应定期对保管的电子档案进行监测，校验电子档案数据的原始性，记录并保存校验结果。

5.2.8 电子档案校验检查应符合GB/T 17710—2008的规定，校验检查可使用完整性校验算法进行设计和实现，电子档案与其副本间执行检查应确保校验结果完全匹配。

5.2.9 电子档案监测结果出现异常，应采用人工或借助电子档案数据保全系统及时修复，确保电子档案的原始性。电子档案的监测、修复过程应形成并保存完整记录。

5.2.10 电子档案在存储过程中如需开展格式转换或存储环境发生变化需要迁移的，应对格式转换过程和迁移过程完整记录。电子档案文件格式转换工作应按5.3要求开展。

# 5.3 电子档案格式转换

5.3.1 格式转换前，应再次进行完整性校验，确保被转换电子档案数据的原始性。转换系统的内置时间应与标准时间同步，并对转换系统实施检查、环境清理和杀毒，确保转换软件的合法性和操作环境的安全性。

5.3.2 格式转换过程中，应生成操作日志或编制操作记录，并用录像、照相、截屏等方式对关键操作步骤进行记录、见证。

5.3.3 应对照转换前的电子档案检查转换后电子档案在内容表达上的完整性、准确性，确保转换前后的电子档案含义一致，形式、功能相当。

5.3.4 格式转换后，应修改并增加与格式转换相关的元数据，并保持电子档案与元数据之间的关联。

5.3.5 转换后的电子档案及其元数据应加以固定。以信息包方式保存的电子档案，通过修改封装包、锁定签名的方式固定；以其他方式保存的电子档案，通过重新计算并存证完整性校验值的方式固定。

5.3.6 格式转换方案、操作日志、一致性检查记录、转换报告等过程相关信息应完备签署，并与格式转换工具一起保存。

# 5.4 电子档案提取出证

5.4.1 电子档案提取应查验申请人的合法身份。电子档案提取出证应经过授权。

5.4.2 提取电子档案，宜同时提取电子档案、电子档案元数据、电子档案附属信息、电子档案存证验证信息。

5.4.3 以离线方式提取，应在拷贝前对移动存储介质进行检查、清理和杀毒，确保载体的安全可靠。

5.4.4 以在线方式提取，应在接入电子存证平台或其他应用系统之前确认数据接口、网络环境和接收系统的安全可靠。

5.4.5 电子档案提取应形成并保存审批记录、申请人身份认证信息和数据提取、传输过程记录。

5.4.6 电子档案提取作为证据提交法院、仲裁等电子数据存证平台或应用系统的，应符合对接部门的要求，提取内容包括5.4.2的要求，并将电子档案生成、归档、存储、保管和提取过程中形成的原始记录及其可信时间标识等一并交付。

# 6 电子档案存证

6.1 具有或潜在法律证据用途的电子档案，应在归档交接之时和格式迁移之后实施存证。

6.2 采用自建或第三方存证平台存证的，存证平台应符合SF/T 0076—2020第5章要求。

6.3 采用电子签名技术方式存证的，被签名对象应为电子档案或电子档案信息包中的被签名对象，签名人为归档移交责任主体，锁定签名人为归档接收责任主体。签名数据不得嵌入电子档案。所用电子签名必须符合《中华人民共和国电子签名法》第三章的要求，电子签名格式应符合GB/T 25064—2010的要求。

6.4 采用加盖时间戳技术方式存证的，应基于国家授时中心授时的可信时间戳服务，可信时间戳服务应符合GB/T 20520—2006规定。加盖时间戳对象为电子档案或电子档案的完整性校验值。时间戳数据不得嵌入电子档案。

6.5 采用完整性校验算法方式存证的，校验对象应为电子档案或电子档案聚合。采用的完整性校验算法应符合国家商用密码算法（SM）的规定。完整性校验值应采用上传区块链或提交可信第三方备验等方式见证或公证。

6.6 其他符合法律或标准要求的电子数据固定和存证技术，在满足合规操作的前提下，可用于实施电子档案的存证。

参考文献

[1]中华人民共和国档案法

[2]中华人民共和国电子签名法

[3]ISO 17068—2017 Trusted third party repository for digital records （可信第三方数字文件仓库）

[4]GB/T 32907—2016 信息安全技术 SM4分组密码算法

[5]GB/T 32918.1—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

[6]GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

[7]GB/T 38635.1—2020 信息安全技术 SM9标识密码算法 第1部分：总则

[8]GB/T 38635.2—2020 信息安全技术 SM9标识密码算法 第2部分：算法

[9]《最高人民法院关于互联网法院审理案件若干问题的规定》