

DB32

江苏省地方标准

DB32/T 5007—2025

电子政务协同办公系统电子文件应用
与管理技术要求

Technical requirements for electronic files application and
management in e-government system

2025-02-06 发布

2025-03-06 实施

江苏省市场监督管理局 发布
中国标准出版社 出版

目 次

前言Ⅲ

1 范围1

2 规范性引用文件1

3 术语和定义2

4 缩略语3

5 总体架构3

6 电子文件应用要求4

 6.1 电子文件4

 6.2 协同办公6

 6.3 档案管理8

 6.4 支撑组件12

7 协同管理要求13

 7.1 管理机构13

 7.2 管理制度14

 7.3 资源管理14

 7.4 运维管理14

 7.5 应急管理14

8 安全防护要求14

 8.1 通用要求14

 8.2 真实性15

 8.3 完整性15

 8.4 可用性16

 8.5 安全性16

 8.6 机密性16

 8.7 不可否认性17

附录A(资料性) 电子政务协同办公系统电子文件应用与管理安全防护映射关系18

附录B(规范性) 电子公文元数据方案19

参考文献28

前 言

本文件按照 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏省工业和信息化厅、江苏省国家密码管理局共同提出。

本文件由江苏省软件和信息技术服务标准化技术委员会归口。

本文件起草单位：江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心）、中共镇江市委办公室、中国电子技术标准化研究院、国泰新点软件股份有限公司、江苏省档案馆、北京金山办公软件股份有限公司、江苏珥仁信息科技有限公司、北京海泰方圆科技股份有限公司、江苏航天七零六信息科技有限公司、北京数科网维技术有限责任公司、南京辰光融信技术有限公司、江苏中威科技软件系统有限公司、扬州万方科技股份有限公司、南京开江科技有限公司、麒麟软件有限公司、常州市档案馆、常州市档案博览中心、常州市国家密码管理局、镇江市国家密码管理局、乾讯信息技术（无锡）有限公司、北京数字认证股份有限公司、江苏意源科技有限公司、江苏信创密码技术有限公司（江苏省密码创新促进中心）、江苏先安科技有限公司、江苏瑞新信息技术股份有限公司、江苏庄科信息技术有限公司、永中软件股份有限公司。

本文件主要起草人：李国琴、张腾标、陈亚军、张树玲、王坤、吴兰、王雷、毛卿、温贤强、安红云、田敬新、金云江、陈万田、徐有法、王平、魏红霞、冯和平、葛文祥、何光辉、马东升、石波、许睿、王少康、张严、张志龙、侯海波、严伟、何中、钱灿军、高正宏、刘伟、缪秋君、杨建军、姜帅、丁余泉、汪晓娟、夏冰冰、陈林、蒋日友、谢吉华、强科华、朱静、庄昱垚、刘雁、卢秋如、徐雁飞、赵玉凤、刘向光、夏建平、蔡蕾、谈辉。

电子政务协同办公系统电子文件应用 与管理技术要求

1 范围

本文件给出了电子政务协同办公系统电子文件应用与管理总体架构,规定了电子政务协同办公系统电子文件应用要求、协同管理要求和安全防护要求。

本文件适用于非涉密电子政务协同办公系统电子文件应用相关的系统建设、协同管理和安全防护过程。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 1988—1998 信息技术 信息交换用七位编码字符集
GB/T 9704—2012 党政机关公文格式
GB/T 13000 信息技术 通用多八位编码字符集(UCS)
GB/T 18894—2016 电子文件归档与电子档案管理规范
GB/T 20273 信息安全技术 数据库管理系统安全技术要求
GB/T 20520 信息安全技术 公钥基础设施 时间戳规范
GB/T 25645 信息技术 中文 Linux 服务器操作系统技术要求
GB/T 29244—2024 网络安全技术 办公设备安全规范
GB/T 33190 电子文件存储与交换格式 版式文档
GB/T 32395 信息技术 中文 Linux 操作系统应用编程接口(API)扩充要求
GB/T 33476.1—2016 党政机关电子公文格式规范 第1部分:公文结构
GB/T 33476.2 党政机关电子公文格式规范 第2部分:显现
GB/T 33476.3 党政机关电子公文格式规范 第3部分:实施指南
GB/T 33477—2016 党政机关电子公文标识规范
GB/T 33478 党政机关电子公文应用接口规范
GB/T 33479 党政机关电子公文交换接口规范
GB/T 33480—2016 党政机关电子公文元数据规范
GB/T 33481 党政机关电子印章应用规范
GB/T 33483 党政机关电子公文系统运行维护规范
GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规则
GB/T 38540 信息安全技术 安全电子签章密码技术规范
GB/T 39362—2020 党政机关电子公文归档规范
GB/T 39784 电子档案管理系统通用功能要求
GB/T 42133—2022 信息技术 OFD 档案应用指南

GB/T 44720 电子文件存储与交换格式 流式文档

DA/T 22—2015 归档文件整理规则

DA/T 31 纸质档案数字化规范

DA/T 47 版式电子文件长期保存格式需求

DA/T 70—2018 文书类电子档案检测一般要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子文件 electronic document

由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。

3.2

电子档案 electronic records

具有凭证、查考和保存价值并归档保存的电子文件。

[来源:GB/T 18894—2016,3.2]

3.3

电子公文 electronic official document

以数字形式存储于磁盘、光盘等媒体,依赖计算机系统阅读、处理并可在通信网络上传输的公文。

[来源:GB/T 33476.1—2016,3.1]

3.4

元数据 metadata

描述电子文件和电子档案的内容、背景、结构及其管理过程的数据。

[来源:GB/T 18894—2016,3.3]

3.5

真实性 authenticity

电子文件、电子档案的内容、逻辑结构和形成背景与形成时的原始状况相一致的性质。

[来源:GB/T 18894—2016,3.5]

3.6

完整性 integrity

电子文件、电子档案的内容、结构和背景信息齐全且没有破坏、变异或丢失的性质。

[来源:GB/T 18894—2016,3.7]

3.7

可用性 availability

电子文件、电子档案可以被检索、呈现或理解的性质。

[来源:GB/T 18894—2016,3.8,有修改]

3.8

安全性 security

通过管理和技术措施保证电子文件、电子档案的应用与管理过程可控,数据存储可靠,未被破坏、未被非法访问的性质。

[来源:DA/T 70—2018,3.7,有修改]

3.9

机密性 confidentiality

保证电子文件、电子档案信息不被泄露给非授权实体的性质。

3.10

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

4 缩略语

下列缩略语适用于本文件。

OCR:光学字符识别(Optical Character Recognition)

OFD:开放版式文档(Open Fixed-layout Document)

OFD-A:开放版式文档档案应用(Open Fixed-layout Document Using in Archive)

PDF:便携式文档格式(Portable Document Format)

SMPC:多方安全计算(Secure Multi-Party Computation)

TLS:安全传输层协议(Transport Layer Security)

UOF:统一办公文档格式(Uniform Office Format)

ZIP:数据压缩文件格式(Zipped Archive)

5 总体架构

电子政务协同办公系统基于支撑组件,通过协同管理和安全防护实现电子文件、协同办公、电子档案的应用与管理过程。电子政务协同办公系统电子文件应用与管理总体架构如图 1 所示,包括协同管理、业务应用、安全防护和支撑组件四部分,具体如下:

- 协同管理主要包括管理机构、管理制度、资源管理、运维管理和应急管理在内的综合管理活动,支撑电子政务协同办公系统电子文件业务应用的安全稳定运行;
- 业务应用主要包括电子文件、协同办公、档案管理三部分,涵盖电子文件形成流转和业务办理、电子文件资源库管理、电子文件预归档管理和电子档案长期保存全过程;
- 安全防护主要包括真实性、完整性、可用性、安全性、机密性和不可否认性,其中,真实性、完整性、可用性和安全性统称四性,保障电子政务协同办公过程以及电子文件和电子档案的真实、完整、可用和安全。电子政务协同办公系统电子文件应用与管理安全防护映射关系见附录 A;
- 支撑组件主要包括应用组件和系统组件。其中,应用组件主要包括支撑电子文件业务应用的流式处理、版式处理、电子签章、全文检索等,系统组件主要包括支撑电子文件业务应用的操作系统、数据库、中间件以及代理组件等。

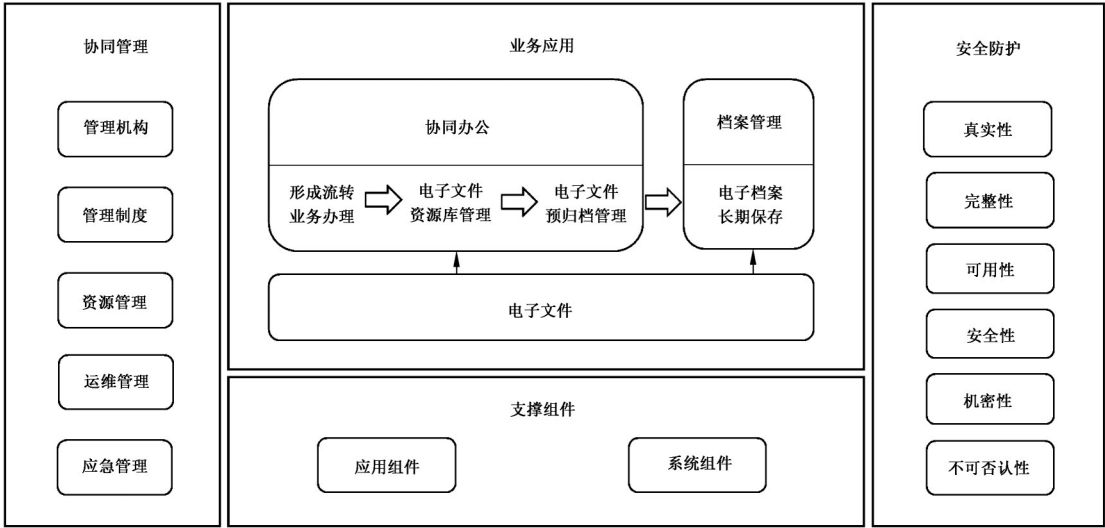


图 1 总体架构

6 电子文件应用要求

6.1 电子文件

6.1.1 通用要求

电子文件通用要求包括：

- a) 电子文件流式文档应按照 GB/T 44720 中规定的要求形成和输出 UOF 格式文件，版式文档应按照 GB/T 33190 中规定的要求输出 OFD 格式文件；
- b) 公文类电子文件应符合 GB/T 33476(所有部分)、GB/T 33477—2016 中规定的要求。

6.1.2 电子文件形成

6.1.2.1 对于系统内部形成的电子文件，电子文件形成要求如下。

- a) 基本能力：
 - 1) 应支持新建文档、编辑文档、文档排版、本地导入功能；
 - 2) 应支持样式设置、页边距设置、分栏设置、页面方向设置、页眉页脚设置；
 - 3) 应支持常用阅读视图，如页面视图、大纲视图、阅读版式、护眼模式；
 - 4) 应提供多种文档内容显示方式，如按页面宽度显示、按百分比缩放显示、按整页显示等；
 - 5) 应支持并排查看功能，可同步滚动所显示的两个不同文档；
 - 6) 应支持插入普通批注、手写批注，实现笔迹留痕功能；
 - 7) 应支持对文本字体格式进行设置，包括但不限于文本字体、字号、颜色、加粗、斜体、下划线和字符间距；
 - 8) 应支持对段落进行编辑和格式设置，包括但不限于对齐方式、大纲级别、文本方向、缩进、行间距和段间距；
 - 9) 应支持对文字表进行编辑和格式设置，包括但不限于新建文字表、设置文字表行高列宽填充等属性、增加或删减文字表行列、删除文字表；
 - 10) 应具备快速添加文字表行列功能，如通过直观的按钮直接增加文字表行和文字表列；
 - 11) 应支持创建常见格式的项目符号列表和编号列表，支持根据输入内容自动识别并创建编号列表，支持多级项目符号列表和编号列表；

- 12) 应具备添加文字和图片两种类型自定义水印、预设水印的功能;
 - 13) 编辑文字文档时,应支持简单的数据运算,利用简单的函数和计算公式实现数据统计和分析;
 - 14) 应具备文档修订、限制编辑、文档审批功能。文档修订时,不同修订人的修订结果应以颜色区分,支持接受、拒绝逐条修订或所有修订;
 - 15) 应支持输入公式,并提供内置常见的数学公式。
- b) 公文能力:
- 1) 应支持符合 GB/T 9704—2012 规定的电子公文页面设置、字体、字号、行间距设置和换行排版规则;
 - 2) 版面要求、格式、式样等各要素编排规则应符合 GB/T 33476.2 中规定的公文逻辑格式要求;
 - 3) 应支持预置公文模板,支持设置公文类型和要素;
 - 4) 应具备公文模板智能转换功能,根据内置国标模板、自定义模板进行一键智能转换公文模板;
 - 5) 应支持公文域功能,支持按照 UOF 标准数据标签要求存储文件;
 - 6) 应支持在公文正文指定位置生成二维条码,公文二维条码的生成、显示见《机关公文二维条码使用规范》;
 - 7) 应支持电子公文写作格式、OFD 文件、截图框选识别区域等场景下的文本识别,快速准确提取文字;
 - 8) 应支持快速识别公文域、分类公文域、快速编辑公文域内容;
 - 9) 应根据电子公文相关要求,具备单个文字或标点符号不单独占用一行功能;
 - 10) 应具备自动缩进对齐功能,保持段落与段落的缩进一致;
 - 11) 应具备公文校对纠错功能,包括但不限于对公文中的错别字、标点、领导人职务及排序、敏感词、叠词、错词等进行纠错;
 - 12) 电子公文所有内容打印后的效果应与编辑时的排版效果一致;
 - 13) 电子公文定稿、修改稿应以带修订标记的 UOF 格式文件形成、存储并归档,宜采用多个带修订标记的流式文档存储法律、法规拟制过程中形成的多版本重要修改稿。
- 6.1.2.2 对于系统外部形成的文件,电子文件形成要求包括:
- a) 系统外部形成的纸质文件应采用符合 GB/T 29244—2024 规定的增强级安全技术要求的扫描设备进行扫描,形成电子文件;
 - b) 扫描形成的电子文件和系统外部的电子文件应保留完整且来源可靠、未被非法更改的元数据;
 - c) 对于扫描后形成的电子文件或系统外部的电子文件,应能够按需转换成流式文档文件,并能够进行编辑等操作。
- 6.1.2.3 电子文件输入输出要求包括:
- a) 应采用符合 GB/T 29244—2024 规定的增强级安全技术要求的输入输出设备;
 - b) 应根据需要提供电子文件防复印、可回溯等功能;
 - c) 应对电子文件输入/输出进行管理和审计。
- 6.1.3 电子文件应用
- 6.1.3.1 电子文件收集要求包括:
- a) 应支持自动采集和手动上传方式;
 - b) 应支持实时对接、定时同步、离线上传等方式;

- c) 应支持多种文件格式数据加工处理,形成电子文件的结构化数据;
- d) 应支持对电子文件中的段落进行关键词标引;
- e) 应支持电子文件确认入库;
- f) 应支持电子文件在不同操作系统平台间迁移与共享,且逻辑格式和内容信息保持完全一致;
- g) 应支持对数字化后的OFD文件进行内容分析以及自动处理。

6.1.3.2 电子文件存储应支持电子文件资源库、主题库、元数据库、业务数据库等的存储。

6.1.3.3 电子文件管理包含文档管理、元数据管理、标签管理和模板管理,包括如下要求。

- a) 文档管理:
 - 1) 应支持电子文件资源库的建立编辑和权限管理;
 - 2) 应支持新建、删除、移动、修改目录以及目录的权限管理;
 - 3) 应支持文档查看、编辑、移动、搜索以及文档的权限管理。
- b) 元数据管理:
 - 1) 应符合GB/T 33480—2016中规定的元数据要求;
 - 2) 应支持按照元数据类别进行分类管理;
 - 3) 应支持对元数据进行搜索。
- c) 标签管理:
 - 1) 应支持新增、删除、编辑和搜索标签;
 - 2) 应支持按照类别进行标签分类,如主题、关键词、实体类别等。
- d) 模板管理:
 - 1) 应支持GB/T 9704—2012中规定的公文模板;
 - 2) 应支持通用模板,如规章、书信、工作计划等。

6.1.3.4 电子文件利用要求包括:

- a) 应支持多端登录电子文件资源库;
- b) 应支持分类检索、关键词检索、语义检索以及元数据检索;
- c) 应支持文件的归集、转化加工、知识化提供利用服务;
- d) 应支持智能推荐、智能检索、智能问答、辅助起草、智能排版和智能校对等功能。

6.2 协同办公

6.2.1 通用要求

协同办公的通用要求包括:

- a) 协同办公应包含公文管理、会议管理、督查督办、请示批示、政务信息、公务邮件和文件交换等业务应用,协同办公过程中的电子文件应用与管理包含公文类电子文件和其他非公文类电子文件管理;
- b) 应结合协同办公实际业务需求,保障协同办公过程中电子文件应用的真实性、完整性、可用性、安全性、机密性和不可否认性;
- c) 电子文件应按照集中存储、空间集约化原则集中存储于电子文件资源库中。

6.2.2 公文类电子文件办公要求

6.2.2.1 处理要求包括:

- a) 公文类电子文件拟制过程包括拟稿、审核、签发等协作环节,应支持对公文类电子文件进行在线编辑、修订留痕、审阅批注、原笔迹签批功能;
- b) 起草、初审、核稿、审签公文类电子文件过程通过协作实现多人同时在线处理的,应确保文件格

式符合电子公文格式要求,且支持编辑、修订留痕、审阅批注、排版、审校功能;

- c) 多人同时在线处理同一个公文类电子文件时,应具备文件冲突检测和顺序处理机制;
- d) 公文类电子文件处理过程应记录文件的中间版本、修订人和修订时间,且修订人与当前用户身份关联;
- e) 公文类电子文件发文办理过程包括复核、登记编号、印制、核发等协作环节,应支持对公文类电子文件进行排版、审校、红头模板套用、添加公文二维条码、转版、盖章功能;
- f) 公文类电子文件收文办理过程包括签收、登记、初审、承办、传阅等环节,应支持对公文类电子文件进行扫描、打印、验章功能;
- g) 公文类电子文件办理流转过程中电子公文处理单模板、电子公文正文模板与电子公文元数据应分离存储。

6.2.2.2 交换要求包括:

- a) 公文类电子文件的交换应包括发送、收回、撤销、签收、退回、反馈、转办等操作;
- b) 公文类电子文件交换的数据类型应包括电子公文元数据、公文正文、附件及交换报文信息,其中公文正文及文本类附件应采用 OFD 格式,并加盖发文单位电子印章;
- c) 公文类电子文件数据交换接口应符合 GB/T 33479 中规定的要求;
- d) 公文类电子文件交换服务端应对数据请求接口进行身份验证,数据传输过程应使用 TLS 1.2 版本及以上或至少同等安全级别的安全通信协议。

6.2.2.3 预归档要求包括:

- a) 协同办公系统应支持公文类电子文件的预归档,预归档包括公文类电子文件的收集、整理、移交过程,并符合 GB/T 39362 中除档案接收外的其他要求;
- b) 归档信息包应包含电子公文元数据、公文处理单、正文主体(包括正本、定稿、中间修订稿、原稿)、附件等文件,其中公文处理单、正文主体及文本类附件应采用 OFD 格式;
- c) 已完成预归档的公文类电子文件应能够通过接口方式将归档信息包与电子文件归档登记表推送到档案管理系统,推送时采用消息队列机制确保推送成功,且支持逐条推送或批量推送方式,接口调用过程应完整记录日志。

6.2.3 非公文类电子文件办公要求

6.2.3.1 会议类电子文件要求包括:

- a) 会议类电子文件管理应涵盖会前、会中、会后整个过程,主要包括会议通知、会议材料(如发言稿、议题材料、议程等)、参会人员名单、签到表、场地布置图、会议纪要、音视频记录、会议信息元数据等相关电子文件,会议通知应采用 OFD 格式并加盖电子印章;
- b) 会议类电子文件的交换应包括发送、收回、撤销、签收、退回、反馈等接口,交换内容主要包括会议信息元数据、会议通知、会议材料、报名表等。

6.2.3.2 督查督办类电子文件要求包括:

- a) 督查督办类电子文件管理应涵盖督办事项登记、下发、反馈和办结的整个过程,主要包括督查通知、督办材料、落实反馈材料、督查督办元数据等相关电子文件;
- b) 督查督办类电子文件交换应包括发送、收回、撤销、签收、退回、反馈、办结等接口,交换内容主要包括督查通知、督办材料、落实反馈材料、督查督办元数据等。

6.2.3.3 内部请示类电子文件管理应涵盖请示事项发起、审核、批示和办结的整个过程,主要包括内部请示件正文、附件、批示件元数据等相关电子文件。

6.2.3.4 政务信息类电子文件要求包括:

- a) 政务信息类电子文件管理涵盖政务信息报送、采用、编辑和发布等过程,主要包括政务信息元数

据、信息报送单、附件、期刊正文、审批处理单等相关电子文件；

- b) 政务信息类电子文件的交换应包括报送、收回、签收、退回等接口,交换内容主要包括政务信息元数据、附件等。

6.2.3.5 公务邮件类电子文件要求包括：

- a) 公务邮件类电子文件应包括公务邮件元数据、邮件详情单、附件等；
- b) 公务邮件类电子文件的交换应包括发送、收回、撤销、签收等接口,交换内容主要包括公务邮件元数据、附件等。

6.2.3.6 协同办公中涉及内部通知、值班上报、信访办理、公务接待、即时通讯、视频会议等其他应用类电子文件要求包括：

- a) 应完整记录文件来源,包括来源应用名称、生成/修改时间、提交人等信息；
- b) 与业务数据建立关联关系,涉及文件修订的应记录修改痕迹并存储修订版本。

6.3 档案管理

6.3.1 通用要求

电子档案管理通用要求包括：

- a) 电子档案管理应包含收集、整理、检测、归档、保管、利用、销毁和档案管理配置；
- b) 电子档案管理系统应符合 GB/T 39362、GB/T 18894 中的功能要求；
- c) 电子公文元数据方案应满足附录 B 中的要求。

6.3.2 档案收集

6.3.2.1 对于系统内部形成的电子文件,收集要求包括：

- a) 在电子文件形成和办理过程中应收集文件及其元数据；
- b) 收集自动捕获的元数据时,应采取技术手段避免人工干预；
- c) 收集手工捕获的元数据时,应根据四性要求和元数据方案对元数据进行校验；
- d) 流式电子文件应在正式盖章前转换成 OFD-A 格式。如无法转换,则将无法转换部分从文件中分离出来作为附件并采用或转成符合长期保存要求的文件格式,其余文件部分转换成 OFD-A 格式；
- e) 所收集的电子文件应支持文档合并、文档拆分功能,便于对文件进行整理。

6.3.2.2 对于系统外部形成的电子文件,收集要求包括：

- a) 通过接口收集文件时,应在收集时按照四性要求和元数据方案对电子文件及其元数据进行检测,检测通过方可接收；
- b) 通过手工收集文件(如著录、上传、导入)时,应在收集时按照四性要求和元数据方案对电子文件及其元数据进行检测,检测通过方可接收；
- c) 对于不符合长期保存要求的电子文件,应在收集前对其进行流式格式(如 UOF)与版式格式(如 OFD)相互转换、文档合并、文档拆分等格式处理,以满足 DA/T 47 中的要求。

6.3.2.3 对于系统外部形成的纸质文件,收集要求包括：

- a) 应使用专业的扫描仪对纸质文件进行扫描,扫描标准符合 DA/T 31 中的要求；
- b) 扫描时应自动捕获数字化相关元数据,扫描成品为三层 OFD-A(元数据层、形式层、内容层)格式,格式符合 GB/T 33190、GB/T 42133、GB/T 39362 中规定的要求；
- c) 扫描时应支持识别文件二维码(适用时),从二维码中提取文件的元数据信息,二维码应符合 GB/T 33476.1—2016 附录 B 中规定的要求。如无二维码,则应由操作员手工著录文件元数据信息；

- d) 系统应将扫描生成的文件标记为“数字化副本”,以便于与原生电子文件进行区分。

6.3.2.4 除满足 6.3.2.1~6.3.2.3 中提及的元数据收集要求外,元数据收集要求还包括:

- a) 应收集公文流转过程中产生的元数据,包括电子文件及其组件标识符、内容与形式特征、物理结构元数据等;
- b) 所收集元数据的类型、值域、格式应符合附录 B 中的要求,方案中约束性为“必选”的元数据应全部收集。

6.3.2.5 组件收集要求包括:

- a) 应按照 DA/T 22—2015 中 5.1 的规定收集电子公文的各个组件并对其进行排序;
- b) 应记录组件的组件类型和组件序号,组件类型可用于标识组件的主次关系,如正文主体(包括正本、定稿、中间修订稿、原稿)、附件、公文处理单、拟稿纸等。其中,组件序号是一个由 1 开始的序号,确保电子公文归档之后各组件的顺序不变。

6.3.2.6 电子公文收集的审计跟踪要求包括:

- a) 应对电子公文收集过程进行全流程审计跟踪,详细记录电子文件及其元数据的收集过程,如收集时间、收集人等,如有变更,则应记录变更时间、变更人等;
- b) 应采用技术手段防范审计跟踪信息被非法篡改;
- c) 协同办公系统应具备追溯功能,能够向前追溯电子文件要素的捕获过程,必要时可通过技术手段保护前后阶段捕获的电子文件要素的一致性。

6.3.3 档案整理

档案整理要求包括:

- a) 应在整理环节对所收集的电子文件组织评审,筛查出无归档价值文件予以删除,对于涉密或含敏感信息的文件,应按照涉密要求处理;对于其余文件,应确定其价值、保管期限等,按照要求进入检测环节;
- b) 系统应支持自动整理功能,按照文件来源、类别、字号、阅办意见等信息进行鉴定分类,符合条件的自动进入检测环节;
- c) 电子公文应按照有关规定使用有业务意义的元数据或元数据组合进行命名。

6.3.4 档案检测

档案检测要求如下。

- a) 应按照 DA/T 70 中规定的检测内容和检测方案对待归档电子公文进行四性检测,检测结束后生成检测报告反馈给用户,检测报告应以 OFD-A 格式保存,归档时随信息包一同在线推送或离线移交到档案管理部门。
- b) 应对待归档电子公文进行真实性检测:
 - 1) 检测元数据准确性,是否与附录 B 中的元数据方案一致;
 - 2) 检测元数据与公文内容的一致性,例如题名、文号、责任者、日期与文件内容是否一致;
 - 3) 检查电子公文的内容准确性,包括文字、数据、图表等是否符合实际情况;
 - 4) 检查电子公文的内容与其他文件或记录的一致性;
 - 5) 检测电子签名是否符合 GB/T 35275 的要求,检测电子印章是否符合 GB/T 38540 的要求,检测数字证书、颁发机构是否符合相关标准要求。
- c) 应对待归档电子公文进行完整性检测:
 - 1) 检查电子公文的内容完整性,包括文件名、文件体、文件尾等部分是否齐全;
 - 2) 检测电子文件组件齐全性,如正文、附件、定稿、带痕迹修改稿、公文处理单、拟稿纸等是否

齐全。

d) 应对待归档电子公文进行可用性检测：

- 1) 检测电子公文文件格式以及电子公文内部所包含的资源是否符合 DA/T 47 中的要求；
- 2) 检测电子公文所使用的字符是否符合 GB/T 13000 中规定的要求，检测版式文件使用的字体是否符合相关标准要求；
- 3) 检测电子公文是否包含加密内容，是否使用非标准压缩算法，是否使用不符合标准规范的数字摘要、电子签名、电子签章，电子签名和电子签章内容是否可读、可解析、可验证；
- 4) 对于标记为“数字化副本”的文件，应检测是否包含数字化元数据，元数据是否符合数字化相关标准要求；
- 5) 应检测文件的扫描质量是否符合数字化相关标准要求；
- 6) 对于 OFD-A 格式的电子公文，还应检测其格式是否符合 GB/T 42133 的要求。如遇到软件无法检测的内容，则应提供界面打开电子文件进行手工检测。

e) 应对待归档电子公文进行安全性检测：

- 1) 检测电子公文文件的安全性，包括文件是否受到保护、是否存在信息泄露风险等；
- 2) 应检测杀毒软件是否是通过国家安全认证或安全检测的产品，杀毒软件病毒库更新日期是否在 3 个月之内；
- 3) 杀毒软件检测出的带病毒电子文件被固化(已经签名或签章)时，应使用技术手段在不破坏文件真实性的情况下进行无害化处理。

6.3.5 档案归档

档案归档要求如下。

- a) 电子公文文件经四性检测后，应由档案管理部门建立文件索引，包括日期、文件名称、编号、主题等信息并进行归档。
- b) 应建立数据定期备份与恢复计划，防止文件丢失或损坏。
- c) 应采取适当的安全措施保护归档文件的安全，防止未经授权的访问和篡改。
- d) 应对归档文件进行定期维护，包括检查文件的完整性、更新索引等。
- e) 对于 OFD-A 格式的电子公文，如果文件内使用的电子签名和电子签章符合 GB/T 42133—2022 中 6.13.1 规定的要求，则可以不作去技术化处理。否则应在归档前对文件内的电子签名和电子签章进行去技术化处理；电子签名和电子签章去技术化处理时应保留原签章的外观和相关属性信息；电子文件去技术化处理后，原件应继续保留作为参考。
- f) 应支持文件归档状态的记录、跟踪和查询。
- g) 采用信息包的方式进行归档时，归档信息包应按照 GB/T 39362—2020 中第 8 章的规定组织，且包含包内电子文件的四性检测报告。
- h) 应支持实时归档和定期归档两种在线归档方式：
 - 1) 归档信息包传输前应使用合规密码技术确认归档源系统和目标系统是否可信；
 - 2) 传输归档信息包时应使用 zip 进行打包，并对信息包进行加密，防止信息泄露；
 - 3) 在线归档时应使用 GB/T 39362—2020 中附录 B.2 定义的接口。接口实现应具备幂等性，并具备单文件推送、多文件批量推送、网络失败重发、归档结果反馈功能；
- i) 应支持离线归档方式：
 - 1) 归档信息包应能够直接保存到存储介质，无须进行打包和压缩，不可对其进行加密；
 - 2) 归档介质应使用档案级光盘或符合长期保存要求的其他存储介质；
 - 3) 当档案管理部门未部署档案管理系统时，归档信息包应包含一份保存电子文件目录的电子

表格。

- j) 协同办公系统与档案管理系统应使用同一套组织架构标准并保持同步,以确保电子文件能够被正确地识别并归入相应的部门。

6.3.6 档案保管

档案保管要求包括:

- a) 应采取技术和管理保障措施,确保电子档案的真实、完整、可用和安全;
- b) 应配套专用设备,确保存储环境的温湿度等物理条件符合保管要求。

6.3.7 档案利用

档案利用要求包括:

- a) 应采取身份认证、权限管理、跟踪审计等安全机制。授权人员根据不同级别访问和操作不同范围的文件区域,通过利用关键词、日期、文件类型等条件进行检索和查询,快速找到需要的文件进行在线阅读,或在审批后进行下载或打印;
- b) 应提供必要的技术手段防范文件利用人员越权下载或打印电子公文;
- c) 应提供必要的功能支持利用人员验证文件电子签名、电子签章的真实性;
- d) 在利用已归档电子文件时应给出适当的标识提示用户;
- e) 应预留 workflow 接口,必要时可在线调取档案管理系统中的已归档电子文件;
- f) 应为电子文件设置开放意见和知悉范围元数据,为电子文件归档后的开放和利用提供建议。

6.3.8 档案销毁

档案销毁要求包括:

- a) 档案销毁前应确保销毁清单经过审批;
- b) 应使用专业工具进行销毁,确保销毁后无法恢复原内容;
- c) 对于存储介质,应委托具备相关资质的机构进行物理销毁,如碾碎、焚烧等;
- d) 档案销毁过程中的申请、审批、销毁清单等记录应予以留存并归档。

6.3.9 档案管理配置

档案管理配置要求包括:

- a) 应建立和维护立档单位信息,支持新增、修改、删除、下载模板、导入/导出、关联档案类型、解除关联绑定和二级立档单位管理功能;
- b) 应根据需要设置门类属性,支持新增、修改、删除、导入和导出功能;
- c) 应具备物理表定义和应用定义功能,应用定义包括列表、界面、检索、排序和档号规则;
- d) 应支持不同功能档案树设置及展示方式,可选择门类节点、全宗节点等树节点;
- e) 应支持对所有表的公共字段进行设置和整理维护;
- f) 应支持为用户提供预置的标准报表样式和自定义个性化报表;
- g) 应支持生成统计源和统计报表,并在前台档案统计模块中展示;
- h) 应能够确定统计定义时的数据源,在统计定义中使用特定表、特定字段等;
- i) 应具备同义词设置功能,能够检索出同一组同义词组中所有同义词相关的档案;
- j) 应具备敏感词库管理功能,在开放鉴定模块中,题名敏感词用红色字体表示。

6.4 支撑组件

6.4.1 通用要求

支撑组件通用要求包括：

- a) 应采用满足国家安全可靠相关规定的支撑组件,保障其功能、性能和安全性满足要求；
- b) 支撑组件中涉及密码算法等密码技术的,应通过授权商用密码检测机构检测并经商用密码认证机构认证合格。

6.4.2 应用组件

应用组件包含流式处理、版式处理、电子签章和全文检索等,其要求如下。

- a) 流式处理：
 - 1) 应支持打开并显示符合 GB/T 44720 中规定的 UOF 格式电子公文；
 - 2) 应支持 GB/T 33476.2 中规定的公文域功能,预置常用公文模板并支持自定义模板；
 - 3) 应支持对电子公文中的表、文、图等要素进行编辑修改；
 - 4) 应支持对公文进行排版,排版效果符合 GB/T 9704—2012 中规定的要求；
 - 5) 应支持将文档按需保存到指定位置；
 - 6) 应支持批注、审阅、修订等功能；
 - 7) 组件接口应符合 GB/T 33478 中规定的二次开发要求。
- b) 版式处理：
 - 1) 应支持打开并显示符合 GB/T 33476.3 中规定的 OFD 格式电子公文；
 - 2) 应支持版式文件与流式文件的相互转换；
 - 3) 应支持对公文添加图文注释、手写批注等功能；
 - 4) 归档文件经转换输出的 OFD 文件应符合 GB/T 33190、GB/T 42133 中规定的要求；
 - 5) OFD 版式软件应满足 GB/T 39784 中规定的功能要求；
 - 6) 应支持实现 OCR 文字识别功能,便于纸质文件的电子化传输、存量档案数字化加工、增量归档文件图片/单层 PDF 等文件内容批量识别并用于全文检索；
 - 7) 应支持提供隐写溯源、水印等安全防护功能；
 - 8) 应支持与电子公文、电子档案、政务服务类应用系统接口互联；
 - 9) 组件接口应符合 GB/T 33478 中规定的二次开发要求。
- c) 电子签章：
 - 1) 应使用由符合 GB/T 33481 要求的应用系统制发的电子印章,支持与江苏省一体化在线政务服务平台统一电子印章系统实现互联互通、互认互信；
 - 2) 应支持符合国家密码应用要求的盖章、验章和信息解析服务；
 - 3) 应支持对 OFD 文件的盖章、验章和印章信息查看功能；
 - 4) 应支持离线验签,实现离线阅读；
 - 5) 组件接口应符合 GB/T 33481 中规定的相关要求。
- d) 全文检索：
 - 1) 应支持通过核心元数据或关键词进行全文检索；
 - 2) 应支持过滤检索、多维分析检索等多种场景的数据检索；
 - 3) 应支持对全部或部分检索结果按照条件排列；
 - 4) 应支持从检索结果中进行检索；
 - 5) 应支持根据人员权限进行检索过滤,不可检索权限范围之外的数据；

- 6) 对于敏感数据,宜支持密文检索。

6.4.3 系统组件

系统组件包含支撑电子文件业务应用相关的操作系统、数据库、中间件以及代理组件等,其要求如下。

- a) 操作系统：
 - 1) 应通过第三方授权测评机构的安全可靠测评；
 - 2) 应符合 GB/T 25645 中规定的技术要求；
 - 3) 应能够适配第三方授权测评机构公布的安全可靠测评结果公告中的处理器；
 - 4) 应支持实现本地部署与虚拟化部署；
 - 5) 应支持各类电子政务协同办公应用的安装、升级、卸载等操作；
 - 6) 接口扩充应符合 GB/T 32395 中规定的要求。
- b) 数据库：
 - 1) 应通过第三方授权测评机构的安全可靠测评；
 - 2) 应符合 GB/T 20273 中规定的技术要求；
 - 3) 应能够适配第三方授权测评机构公布的安全可靠测评结果公告中的处理器与操作系统；
 - 4) 应支持根据电子公文类型建立基础库与主题库；
 - 5) 应支持与密码产品、安全产品对接,实现数据安全防护。
- c) 中间件：
 - 1) 应能够适配第三方授权测评机构公布的安全可靠测评结果公告中的处理器、操作系统与数据库；
 - 2) 应支持为电子公文、电子档案、政务服务等应用系统提供基础支撑。
- d) 代理组件：
 - 1) 应能够适配第三方授权测评机构公布的安全可靠测评结果公告中的处理器、操作系统与数据库；
 - 2) 应实现各类应用系统间的解耦；
 - 3) 应支持灵活的部署方式和简单的配置方式。

7 协同管理要求

7.1 管理机构

管理机构要求包括：

- a) 应成立指导和管理电子政务协同办公系统电子文件应用与管理安全工作的领导小组或委员会,主要负责人由单位主管领导担任或授权；
- b) 应设立电子政务协同办公系统电子文件应用与管理安全工作的职能部门及安全管理负责人,并明确安全管理负责人职责；
- c) 应设立系统管理员、网络管理员、审计管理员、安全管理员、密码管理员、内容审核员、电子文件管理员、档案管理员等岗位,并定义各个工作岗位职责；
- d) 应确保安全管理员为专职人员,不可兼任；
- e) 应建立与网络和数据安全管理部门、职能部门、安全组织、供应商和业界专家等的联系名录,加强内外部的合作与沟通。

7.2 管理制度

管理制度要求包括：

- a) 应建立由安全策略、管理制度、操作规程、记录表单等构成的安全管理制度体系；
- b) 应根据电子政务协同办公系统协同办公应用、文件资源利用、档案管理应用全生命周期制定安全管理制度体系；
- c) 应通过正式、有效的方式发布安全管理制度，并进行版本控制；
- d) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7.3 资源管理

资源管理要求包括：

- a) 应严格规范人员录用和离岗过程，对被录用人的身份、背景、专业资格和资质等进行审查，必要时对其所具有的技术技能进行考核；人员离岗时进行安全审查以确保人员离岗信息安全；
- b) 应与关键或重要岗位人员签署保密协议；从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；
- c) 应制定年度培训计划并进行人员培训，确保人员在知识、技能、经验和安全意识等方面满足岗位运行要求，定期实施人员绩效考核或能力评价；
- d) 应采用安全技术措施保障电子政务协同办公系统协同办公应用、文件资源利用、档案管理应用全生命周期安全；
- e) 应提供合理及适度的资金投入，以确保电子政务协同办公系统电子文件应用与管理业务应用的安全可靠运行。

7.4 运维管理

电子政务协同办公系统电子文件应用与管理运维管理规范应符合 GB/T 33483 中规定的要求。

7.5 应急管理

应急管理要求包括：

- a) 应根据电子政务协同办公系统协同办公应用、文件资源利用和档案管理应用具体特点，按照国家和行业主管部门要求制定统一的应急响应预案框架，至少包含总则、组织架构、角色及职责、预防和预警机制、启动条件、响应分级、处置流程及资源保障等内容；
- b) 应制定网络和数据安全事件报告及处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
- c) 应定期组织实施网络和数据安全事件应急演练活动，并根据演练情况修订完善应急预案；
- d) 网络和数据安全事件发生时，应按照应急预案及时组织应急处置和记录，并进行信息报送；
- e) 应建立应急值班制度，安排专人通过电话、邮件等方式进行监控，定期进行信息报送。

8 安全防护要求

8.1 通用要求

电子政务协同办公系统电子文件应用与管理在网络安全、数据安全、系统安全等方面的通用安全防护应符合国家相关技术标准和管理规范要求，具体要求包括：

- a) 采取与系统安全级别相匹配的安全管控机制和技术措施，确保电子文件、电子档案在全生命周

期各环节的真实性、完整性、可用性和机密性,避免文件被未授权访问、破坏、篡改、泄露或丢失等;

- b) 根据软件技术发展、网络环境变化及时优化电子文件、电子档案的安全控制策略和安全防护措施;
- c) 所采用的电子签名、电子签章、时间戳等密码技术应分别符合 GB/T 35275、GB/T 38540、GB/T 20520 等标准中的要求;
- d) 凡使用对称密码算法、非对称密码算法和密码杂凑算法时,应采用满足国家密码管理部门批准的商用密码算法;
- e) 应采用成熟的安全技术或部署通过国家安全认证或安全检测的安全产品进行安全防护,安全级别符合国家网络安全等级保护和商用密码应用安全等要求。

8.2 真实性

通过采用数字证书、电子签名、电子印章等密码技术保障协同办公应用、电子文件应用和电子档案管理在收集、整理、检测、归档、保管和利用过程中的真实性。具体要求包括:

- a) 应根据四性检测要求保证电子文件和电子档案内容数据的电子属性与元数据中所记录的电子属性的关联一致性;
- b) 应根据四性检测要求保证电子文件和电子档案内容数据与目录数据之间的关联一致性,以及元数据与目录数据标注的一致性;
- c) 应采用强密码策略和多因素身份验证等措施实施身份鉴别,确保电子文件、电子档案协同流转处理过程中访问主体、客体以及接口认证双方身份的真实性;
- d) 应采用访问控制机制对电子文件和电子档案的操作权限进行限制,保证只有经过授权的用户可以访问、修改或更新关联信息;
- e) 应采用密码技术保护电子政务协同办公系统中的重要文件数据,防止意外或恶意的修改或篡改;
- f) 应采用数字证书、数字摘要、电子签名等密码技术验证电子文件和电子档案的来源真实性,确保其由可信的来源创建或收集;
- g) 宜采用可信时间戳技术为电子文件和电子档案提供时间证明,确保电子文件和电子档案在特定时间点的存在性和内容的完整性。

8.3 完整性

通过采取安全防护措施保障协同办公应用、电子文件应用和电子档案管理在收集、整理、检测、归档、保管和利用过程中信息的完整性,同时采用检测技术对电子文件、电子档案的内容进行完整性检测,防止在协同办公、电子文件管理和电子档案管理过程中重要数据被篡改,确保信息的完整性。具体要求包括:

- a) 应采用访问控制机制,限制对文件的修改权限,只允许经过授权的用户进行修改操作,防止未经授权访问和篡改访问控制信息,并对文件的读取和修改行为进行记录,以便追踪和审计可能的安全事件;
- b) 应采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术对电子文件业务应用中的重要数据进行完整性保护;
- c) 应采用冗余校验、奇偶校验等数据校验机制,检测和纠正元数据项的错误或损坏,同时在电子文件和电子档案接收、管理归档和长期保存环节进行完整性检测;
- d) 应在电子文件和电子档案关联过程中进行关联数量的比对,确保关联的文件数量与预期一致,防止数据丢失或重复关联,确保电子文件、电子档案的完整性;

- e) 应确定电子文件归档的范围,确保所有相关的文件都被正确归档,不遗漏任何重要文件或信息;
- f) 应定期进行档案目录和索引的比对,以验证归档范围的完整性,并及时调整和修复可能的错误。

8.4 可用性

通过采取安全防护措施保障协同办公应用、电子文件应用和电子档案管理在收集、整理、检测、归档、保管和利用过程中可以被合法用户正常获取或访问,防止电子文件和电子档案无法使用。具体要求包括:

- a) 应使用符合相关标准要求的文件格式和编码,确保电子文件、电子档案在不同平台和应用程序中能够被正确读取;
- b) 应采用电子文件、电子档案异质备份存储机制,定期进行检查,确保电子文件、电子档案无丢失或未损坏;
- c) 应配置防火墙和入侵检测系统等安全设备并进行定期维护和更新,保护系统免受未经授权的访问和攻击;
- d) 应定期进行系统和应用程序的性能测试和优化,确保其响应时间和吞吐量满足用户需求;
- e) 应采用监控和日志审计机制,及时检测 and 解决潜在的可用性问题;
- f) 应采用容错和备份机制防止单点故障,确保资源服务的稳定性和高可用性,在系统和应用程序出现故障时能够迅速恢复并继续提供服务。

8.5 安全性

通过采取安全防护措施保障电子文件、电子档案形成、移交、归档、存储等过程安全,以及协同办公应用、电子文件应用和电子档案管理计算存储等支撑系统运行环境安全。具体要求包括:

- a) 应建立身份验证和访问控制机制,限制对存储和计算资源、归档和移交文件的访问权限,避免未授权的访问和操作;
- b) 应实施加密传输和存储,确保归档和转交过程中的数据传输和存储安全;
- c) 应部署安全有效的防病毒软件和安全补丁,定期对电子文件、电子档案及其系统环境进行病毒扫描查杀;
- d) 应加强网络隔离和应用安全控制策略,防止恶意软件通过文件传播和感染系统;
- e) 应确保存储系统和计算环境安全性,定期实施安全策略检查更新和漏洞扫描修复;
- f) 应启用系统日志和审计功能以便后续审计和追踪,记录电子文件和电子档案处理过程中的操作行为,定期审查日志记录,及时发现异常操作和安全风险并及时进行告警和处置;
- g) 应通过应用加固等方式确保移动端应用运行环境安全,涉及具体政务工作的电子文件应遵循不落地原则,只提供文件预览,不提供下载;
- h) 应设立安全规范和标准操作流程,加强员工的安全意识培训,指导员工在文件处理和存储过程中遵循安全最佳实践,避免信息泄露。

8.6 机密性

通过采取安全防护措施保障电子政务协同办公系统中的身份鉴别信息、密钥数据、重要文件数据的机密性,确保电子文件、电子档案只能被授权人员访问和操作。具体要求包括:

- a) 应采用安全通信协议实现通信信道加密传输,确保重要数据在传输过程中的机密性;
- b) 应对包含重要数据的电子文件和电子档案进行加密存储,确保重要数据在存储过程中的机密性;
- c) 应确保密钥的安全存储和管理,避免密钥泄露导致电子文件和电子档案数据被恶意获取;

- d) 应制定脱敏策略和规则对敏感信息进行脱敏处理,确保敏感信息的机密性;
- e) 应建立细粒度的访问控制策略,基于最小权限原则,根据用户角色和需求设置对重要数据的访问权限,确保只有经过授权的用户可以访问;
- f) 必要时,可使用安全多方计算(SMPC)、同态加密等隐私计算技术或数据安全沙箱技术等对数据进行加密处理,保护敏感个人信息,在不暴露原始数据的情况下进行数据分析和计算,确保敏感个人信息的机密性;
- g) 应对移动端处理的电子文件进行加密,并采用水印、防截屏等方式防止信息泄露。

8.7 不可否认性

通过采用电子印章、时间戳等安全防护措施保障电子政务协同办公应用在协同协作、流转处理等过程中数据原发行为的不可否认性和数据接收行为的不可否认性。具体要求包括:

- a) 针对可能涉及法律责任认定的电子文件、电子档案,在生成或修改时,应使用数字签名或电子印章等密码技术进行数字签名或签章,并记录签名者或签章者、时间戳等相关信息,确保数字签名或签章操作行为的不可否认性;
- b) 应采用身份鉴别等安全认证技术,确保电子文件数据发送者、接收者身份的真实性;
- c) 接收文件时,应对电子文件的数字签名进行验证,确认其来源真实性和完整性;
- d) 应记录和保存重要操作日志,并采用合规密码技术对其进行完整性保护,确保在需要时能够提供追溯和审计。

附 录 A
(资料性)

电子政务协同办公系统电子文件应用与管理安全防护映射关系

电子政务协同办公系统电子文件应用与管理安全防护映射关系如表 A.1 所示。

表 A.1 电子政务协同办公系统电子文件应用与管理安全防护映射关系表

业务应用		安全防护					
		真实性	完整性	可用性	安全性	机密性	不可否认性
电子文件	收集	✓	✓	✓	✓	✓	—
	存储	✓	✓	✓	✓	✓	—
	管理	✓	✓	✓	✓	✓	—
	利用	✓	—	✓	✓	✓	—
协同办公	公文	✓	✓	✓	✓	✓	✓
	会议	✓	✓	✓	✓	✓	—
	督查督办	✓	✓	✓	✓	✓	—
	内部请示	✓	✓	✓	✓	✓	—
	政务信息	✓	✓	✓	✓	✓	—
	公务邮件	✓	✓	✓	✓	✓	—
	其他	✓	—	✓	✓	—	—
档案管理	收集	✓	✓	✓	✓	✓	✓
	整理	✓	✓	✓	✓	✓	✓
	检测	✓	✓	✓	✓	✓	—
	归档	✓	✓	✓	✓	✓	✓
	保管	✓	✓	✓	✓	✓	—
	销毁	—	—	—	—	✓	✓

附 录 B
(规范性)
电子公文元数据方案

B.1 公文标识

中文名称:公文标识;
定义:等同于电子文件号,电子公文的唯一标识,以区别于其他公文;
英文名称:Document_Identifier;
数据类型:字符型;
值域:符合 GB/T 33477—2016 的要求;
短名:GWBS;
注解:必选;
取值示例:1.2.156.10.1210000400002195R-000-2016-0A-00056-X。

B.2 标题(题名)

中文名称:标题;
定义:对公文主要内容的概括。一般由发文机关名称、事由和文种组成;
英文名称:Document_Title;
数据类型:字符型;
值域:不作要求;
短名:BT;
注解:必选;
取值示例:××部关于开展“××××推进专项行动”的通知。

B.3 成文日期

中文名称:成文日期;
定义:会议通过或者发文机关负责人签发的日期。联合行文时,署最后签发机关负责人签发的日期;
英文名称:Issued_Date_of_Document;
数据类型:字符型;
值域:八位阿拉伯数字;
短名:CWRQ;
注解:必选;
取值示例:20160415。

B.4 发文字号(文号)

中文名称:发文字号;
定义:由发文机关代字、年份和发文顺序号组成;
英文名称:Issued_Number_of_Document;

数据类型:字符型;

值域:含发文机关代字、年份和发文顺序号,其中年份由4位阿拉伯数字组成,用中括号括入,发文顺序号为正整数,多个文号之间“;”分隔;

短名:FWZH;

注解:必选;

取值示例:××发〔2016〕10号。

B.5 密级和保密期限

中文名称:密级和保密期限;

定义:公文秘密等级和保密的期限;

英文名称:Security_Classification_and_Duration;

数据类型:字符型;

值域:密级可取值为绝密、机密、秘密或无;保密期限可取值为时长(年、月、日或“长期”),或解密条件的描述;密级在前,保密期限在后;中间添加分隔符的,应使用★;

短名:MJBMQX(或MJ);

注解:必选;

取值示例:机密★20年;秘密★6个月;机密★长期;机密★××会前。

B.6 签发人(签发人署名)

中文名称:签发人;

定义:签发公文的人的姓名;

英文名称:Signer;

数据类型:字符型;

值域:多个签发人姓名之间以“;”分隔;

短名:QFR;

注解:必选;

取值示例:张××;李××。

B.7 发文单位(责任者)

中文名称:发文单位;

定义:发文机关的全称或规范化简称;

英文名称:Signature_of_Document_Issuing_Agency;

数据类型:字符型;

值域:不作要求;

短名:FWJG;

注解:可选;

取值示例:××市政府。

B.8 发文机关标志

中文名称:发文机关标志;

定义:发文机关全称或者规范化简称,其后添加特定标志;

英文名称:Identification_of_Document_Issuer;

数据类型:字符型;

值域:不受限制,发文机关是发文机关全称或者规范化简称,每个机关名称的长度原则上不超过50个字;不同发文机关之间以“^”(GB/T 1988—1998规定的编码为5E)分隔,如有标志,在最后一个发文机关后加2个“^”及标志;公文文件的标志取值为“文件”或不带标志;纪要文件的标志取值为“××××纪要”;命令的标志取值为“命令”或“令”;不能明确划归为发文机关名称的内容归为标志;

短名:FWJGBZ;

注解:可选;

取值示例:××市委^××市政府^^文件;××市政府^^令;^^××会议纪要。

B.9 主送机关

中文名称:主送机关;

定义:公文的主要受理机关。应使用主送机关的全称或规范化简称或者同类型机关的统称;

英文名称:Main_Receiver_Department;

数据类型:字符型;

值域:多个单位时以“;”分隔;

短名:ZSJG;

注解:可选;

取值示例:××市政府办公厅;××市委办公厅。

B.10 抄送机关

中文名称:抄送机关;

定义:除主送机关外需要执行或者知晓公文内容的其他机关;

英文名称:Copy_to_Department;

数据类型:字符型;

值域:多个单位时以“;”分隔;

短名:CSJG;

注解:可选;

取值示例:××市政府办公厅;××自治区政府办公厅;各人民团体。

B.11 印发机关

中文名称:印发机关;

定义:公文的送印机关,一般是各机关的办公厅(室)或文秘部门;

英文名称:Printing_and_Sending_Department;

数据类型:字符型;

值域:不作要求;

短名:YFJG;

注解:可选;

取值示例:××部办公厅。

B.12 印发日期

中文名称:印发日期;
定义:公文的送印日期;
英文名称:Printing_Date;
数据类型:字符型;
值域:八位阿拉伯数字;
短名:YFRQ;
注解:可选;
取值示例:20160415。

B.13 文种

中文名称:文种;
定义:公文的种类;
英文名称:Document_Type;
数据类型:字符型;
值域:命令(令)、决定、公告、通告、通知、通报、议案、报告、请示、批复、意见、函、会议纪要、公报、决议、其他、保留;
短名:WZ;
注解:可选;
取值示例:通告。

B.14 份号

中文名称:份号;
定义:公文印制份数的顺序号;
英文名称:Serial_Number_of_Copies;
数据类型:数字型;
值域:六位阿拉伯数字;
短名:FH;
注解:可选;
取值示例:000001。

B.15 紧急程度

中文名称:紧急程度;
定义:对公文送达和办理的时限要求;
英文名称:Emergency_Degree;
数据类型:字符型;
值域:公文的紧急程度取值为特急、加急;电报的紧急程度取值为特提、特急、加急、平急;
短名:JJCD;
注解:可选;
取值示例:特急。

B.16 附件说明

中文名称:附件说明;
定义:公文附件的顺序号和名称;
英文名称:Attachment;
数据类型:字符型;
值域:不同附件说明之间以“;”分隔;
短名:FJSM;
注解:可选;
取值示例:关于××××情况的调查报告;关于××××事宜的建议方案。

B.17 附注

中文名称:附注;
定义:公文印发传达范围等需要说明的事项;
英文名称:Annotation;
数据类型:字符型;
值域:不作要求;
短名:FZ;
注解:可选;
取值示例:此件属工作秘密。

B.18 发布层次

中文名称:发布层次;
定义:公文允许传达的范围;
英文名称:Release_Level;
数据类型:日期型;
值域:公文的发布层次,可取值“公开发布”“特定范围”等;
短名:FBCC;
注解:可选;
取值示例:公开发布。

B.19 拟稿人

中文名称:拟稿人;
定义:拟稿人员称谓;
英文名称:Draftsman;
数据类型:字符型;
值域:不作要求;
短名:NGR;
注解:可选;
取值示例:张三。

B.20 移交人

中文名称:移交人;
定义:档案移交人员称谓;
英文名称:Transferor;
数据类型:字符型;
值域:不作要求;
短名:YJR;
注解:可选;
取值示例:张三。

B.21 档号

中文名称:档号;
定义:以字符形式赋予档案(电子文件)的用以固定和反映档案(电子文件)排列顺序的一组代码;
英文名称:Archival_Code;
数据类型:字符型;
值域:本单位自行生成的档号;
短名:DH;
注解:必选;
取值示例:3101-WS2022-Y-BGS-0001。

B.22 年度

中文名称:年度;
定义:电子文件按年度分类后标记形成的处理年度;
英文名称:Year;
数据类型:字符型;
值域:四位阿拉伯数字;
短名:ND;
注解:必选;
取值示例:2009。

B.23 保管期限

中文名称:保管期限;
定义:对电子文件划定的存留年限以字母数字表示;
英文名称:Retention_Period;
数据类型:字符型;
值域:Y、D30、D10;
短名:BGQX;
注解:必选;
取值示例:D30。

B.24 件号

中文名称:件号;
 定义:档案室(馆)编制文件或组合文件的排列顺序号;
 英文名称:Item_Number;
 数据类型:字符型;
 值域:四位阿拉伯数字;
 短名:JH;
 注解:必选;
 取值示例:0001。

B.25 数字对象标识

中文名称:数字对象标识;
 定义:应逐一著录一份电子档案中每个文件的编号,中间用“;”分割;
 英文名称:Electronic_File_Identifier;
 数据类型:字符型;
 值域:
 发文:正本、发文稿纸、定稿、表单、历次修改稿、附件等;
 收文:办文单、正本、表单、复函/办件、附件等;
 按以上顺序以“档号—序号”格式命名各个文件;序号三位数字对齐,从1开始;
 短名:SZDXBZ;
 注解:必选;
 取值示例:档号-001.ofd;档号-002.ofd。

B.26 档案门类代码

中文名称:档案门类代码;
 定义:采用《中国档案分类法》对电子文件进行主题分析,并依照电子文件的内容和特点分门别类后形成的类目标记符号;
 英文名称:Archives_Catalogue;
 数据类型:字符型;
 值域:参考《省级机关团体企业事业单位进馆档案分类编号规范》;文书类电子文件取值为:WS;
 短名:DAMLDM;
 注解:必选;
 取值示例:WS;KJ;KU。

B.27 机构或问题代码

中文名称:机构或问题代码;
 定义:对电子文件进行分类整理时按部门或问题分类的结果;
 英文名称:Organization_or_Function;
 数据类型:字符型;
 值域:各单位自行编制三位字符,例如BGS(办公室)、RSC(人事处);

短名:JGWTDM;

注解:必选;

取值示例:BGS。

B.28 公开属性

中文名称:公开属性;

定义:电子文件对外公开的意见;

英文名称:Disclosure_Attribute;

数据类型:字符型;

值域:主动公开、依申请公开、不予公开;

短名:GKSX;

注解:必选;

取值示例:主动公开;依申请公开;不予公开。

B.29 开放标识

中文名称:开放标识;

定义:标志电子文件是否公开的标识符;

英文名称:Opening_Identification;

数据类型:字符型;

值域:开放、控制、延期开放、未审核;

短名:KFBS;

注解:可选;

取值示例:开放。

B.30 页数

中文名称:页数;

定义:电子文件的页数,包括封面、封皮;

英文名称:Number_of_File_Pages;

数据类型:字符型;

值域:通过系统自动捕获 OFD 或 PDF 文件的页数;

短名:YS;

注解:可选;

取值示例:18。

B.31 备注

中文名称:备注;

定义:需要特别说明的事项;

英文名称:Remark;

数据类型:字符型;

值域:不作要求;

短名:BZ;

注解:可选;
取值示例:——。

B.32 文件属性

中文名称:文件属性;
定义:文件是原生电子文件还是数字化副本;
英文名称:File_Attribute;
数据类型:字符型;
值域:电子文件、数字化副本;
短名:WJSX;
注解:可选;
取值示例:电子文件。

B.33 数字对象类型

中文名称:数字对象类型;
定义:电子文件所包含的数字对象的类型;
英文名称:Electronic_File_Type;
数据类型:字符型;
值域:正文、附件、定稿、带痕迹修改稿、公文处理单、拟稿纸;
短名:SZDXLX;
注解:可选;
取值示例:正文。

B.34 数字对象序号

中文名称:数字对象序号;
定义:数字对象在电子文件内的顺序号;
英文名称:Electronic_File_Order;
数据类型:数字型;
值域:正整数;
短名:SZDXXH;
注解:可选;
取值示例:1。

参 考 文 献

- [1] GB/T 25647 电子政务术语
 - [2] GB/T 34079.4 基于云计算的电子政务公共服务平台服务规范 第4部分:应用服务
 - [3] GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求
 - [4] GB/T 39786 信息安全技术 信息系统密码应用基本要求
 - [5] GM/T 0055 电子文件密码应用技术规范
 - [6] GM/T 0071 电子文件密码应用指南
 - [7] DA/T 46 文书类电子文件元数据方案
 - [8] 机关公文二维条码使用规范(中秘文发[2005]56号)
 - [9] 电子文件管理暂行办法(中办 国办 厅字[2009]39号)
 - [10] 党政机关公文处理工作条例(中办发[2012]14号)
 - [11] 政务服务电子文件归档和电子档案管理办法(国办发[2023]26号)
 - [12] 电子公文归档管理暂行办法(国家档案局令第6号)
 - [13] 电子档案管理办法(国家档案局令第22号)
 - [14] 安全可靠测评工作指南(试行)(中国信息安全测评中心)
 - [15] 省级机关团体企业事业单位进馆档案分类编号规范(苏档馆发[2022]67号)
-