ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

人事档案全生命周期安全管控规范

Specification for Full Life Cycle Safety Control of Personnel Archives

（工作组讨论稿）

（本草案完成时间：2026 - 5 - 6 ）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

人事档案全生命周期安全管控规范

1 引言

为深入贯彻落实《“十四五”全国档案事业发展规划》关于推进档案治理体系和治理能力现代化的核心部署，全面落实总体国家安全观，筑牢人事档案安全防线，夯实国家人才资源管理基础，特制定本文件。当前，我国人事档案管理领域仍存在收集不完整、流转不可控、数字化安全隐患突出、利用权限界定模糊等共性问题，严重影响人事档案的真实性、完整性、可用性和机密性，制约国家人才管理效能提升。本文件严格依据《中华人民共和国保守国家秘密法》《中华人民共和国档案法》及国家最新法律法规、行业标准，整合广西产学研科学研究院在标准化领域的实践成果与全国多地先进管理经验，构建覆盖人事档案“形成、流转、保存、利用、销毁”全生命周期的闭环管控体系，为各级各类组织开展人事档案安全管理工作提供科学、规范、可落地、可追溯的国家级指导依据，助力推动全国人事档案管理工作标准化、规范化、数字化、安全化发展，服务国家人才强国战略与治理体系现代化建设。

2 范围

明确了人事档案全生命周期安全管理的核心要求，规定了人事档案安全风险评估、基础设施安全、全流程管控（收集、流转、整理、保管、利用、销毁）及应急处置的技术标准、管理规范和责任要求，覆盖人事档案管理各环节、各主体、各载体。适用于中国共产党各级机关、各级人民政府机关、国有企业、事业单位、社会团体及各级各类组织的人事档案安全管理工作，涵盖在职人员、离退休人员、流动人员等各类群体的人事档案，为全国人事档案安全管理提供统一遵循，推动形成上下联动、标准统一、管控严密的人事档案安全管理格局。

3 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 9704-2012 党政机关公文格式

GB/T 11821-2002 照片档案管理规范

GB/T 11822-2008 科学技术档案案卷构成的一般要求

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 28827.1-2022 信息技术服务运行维护第 1 部分：通用要求

GB/T 31490.1-2015 电子档案存储用光盘标识

GB/T 33190-2016 电子文件存储与交换格式版式文档

GB/T 33476.1-2016 党政机关电子印章应用规范

GB/T 33870-2017 干部人事档案数字化技术规范

GB/T 34832-2017 信息与文献文件管理过程文件元数据

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 39335-2020 信息安全技术个人信息安全影响评估指南

GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

GB/T 41512-2022 纸质档案数字复制件光学字符识别（OCR）技术规范

GB/T 42727-2023 政务服务事项电子文件归档规范

DA/T 1-2000 档案工作基本术语

DA/T 12-2012 全宗卷规范

DA/T 18-2022 档案著录规则

DA/T 31-2017 纸质档案数字化技术规范

DA/T 38-2021 电子文件归档与电子档案管理规范

DA/T 68-2022 档案服务外包工作规范

LD/T 04-2020 流动人员人事档案安全管理规范

DA/T 81-2019 档案库房空气质量检测技术规范

ISO 15489-1:2016 信息与文献 文件管理

《中华人民共和国保守国家秘密法实施条例》（2024 年修订）

4 术语和定义

GB/T 33870-2017、LD/T 04-2020 界定的以及下列术语和定义适用于本文件。

4.1 人事档案全生命周期

指人事档案从文件材料形成、收集、整理、保管、利用、转递到最终销毁或永久保存的完整过程，是人事档案管理的核心主线，贯穿人才管理全过程，事关国家人才信息安全与历史真实记录。

4.2 安全管控

指遵循总体国家安全观，通过技术手段、管理措施和制度保障，确保人事档案在物理实体、信息内容、利用权限等方面全面满足真实性、完整性、可用性、机密性要求的常态化管控状态，是维护人事档案安全的核心举措。

4.3 三员分立

指在人事档案数字化管理系统中，严格设置系统管理员、安全保密管理员、安全审计员三个相互独立、相互制约的岗位角色，落实岗位分离、权责明晰的管理要求，防范数字化管理中的安全风险，保障系统安全规范运行。

5 总体安全要求

5.1 安全方针

各级各类组织应牢固树立总体国家安全观，建立“预防为主、全程管控、责任到人、科技强安、从严管控”的档案安全管理方针，将人事档案安全工作纳入单位总体安全工作布局，贯穿人事管理和档案管理全过程，确保人事档案安全万无一失。

5.2 风险评估

应至少每 12 个月组织一次全面的人事档案安全风险评估，重大人事变动、机构调整或系统升级后应及时开展专项评估。评估工作严格依据 GB/T 39335-2020 及《中华人民共和国保守国家秘密法实施条例》相关要求执行，重点识别收集、流转、利用等关键环节中存在的泄露、篡改、丢失、损毁等安全风险，建立风险清单、明确防控措施、落实整改责任，形成完整的风险评估报告并归档留存，实现风险闭环管理。

5.3 经费保障

各单位应高度重视人事档案安全保障工作，按档案数量及年增长量，按不低于每万卷人民币 4 万元/年的标准，设立档案安全专项经费，实行专款专用、单独核算。经费主要用于库房维护、安全设备更新、数字化建设与外包、灾备体系建设、安全培训、应急处置等工作，保障人事档案安全管理工作有序

开展，确保安全投入与管理需求相匹配，夯实人事档案安全保障基础。

6 物理环境与基础设施安全

6.1 库房选址与建筑

档案库房选址应符合国家档案库房建设相关标准，严禁设置在地下室、顶层或易受自然灾害影响的区域，其地面承重能力应不小于档案装具满载后的实际荷载且不低于 12kN/㎡。库房应严格实行与办公室、阅览室、数字化加工间“三分开”管理，杜绝交叉干扰；门体采用甲级防火防盗门，窗户配备防盗、防光、防尘设施，库房墙体、地面、天花板应具备防火、防潮、防渗功能，从硬件层面筑牢物理安全防线。

6.2 环境控制

6.2.1 温湿度：保存纸质档案的库房，温度应严格控制在 14℃～24℃之间，日变化幅度不超过±2℃；相对湿度应控制在 45%～60%之间，日变化幅度不超过±5%。应配备智能温湿度调控设备，实现实时监测、自动调控，每昼夜温湿度监测记录不少于 2 次，确保温湿度始终处于标准范围，防范档案霉变、虫蛀、纸张老化等问题。

6.2.2 空气净化：库房空气污染物浓度应严格符合 DA/T 81-2019 要求，颗粒物浓度 PM10 不应超过 0.10mg/m³，二氧化硫浓度不应超过 0.01mg/m³。应配备空气净化设备，定期开展空气检测与净化处理，建立空气质量监测档案，保障档案保存环境安全。

6.2.3 防害：库房应全面具备防水、防光、防虫、防鼠、防磁（针对磁介质档案）功能。防光措施应满足紫外线照度控制在 750 勒克斯（Lux）以下，避免档案纸张、字迹褪色老化；配备符合标准的防虫、防鼠药品，定期检查更换；磁介质档案应单独存放于防磁柜，防范磁场干扰造成数据丢失。

6.3 数字化加工场所

开展档案数字化加工的现场，应设置为独立封闭区域，与其他区域物理隔离，安装 360°无死角高清视频监控系统，视频数据保存时间不少于 6 个月，实现加工全过程可追溯。严格执行出入登记制度，严禁携带手机、相机等具有摄像、存储功能的电子设备进入加工区域，加工设备实行专人管理、专用专用，严禁接入互联网，防范数字化加工过程中的信息泄露风险。

7 归档与收集安全

7.1 归档时限

人事变动（如入职、离职、升职、奖惩、调动）发生后，相关人事材料应在 60 个自然日内完成归

档，确保档案信息及时更新。其中，学历变更、资格认证、职称评定、工资调整等涉及个人核心权益的材料，自办理完毕之日起 30 个工作日内必须移交归档，严禁拖延、遗漏，保障人事档案信息的时效性和完整性。

7.2 材料接收

档案管理人员在接收人事材料时，应严格履行审核职责，逐一检查材料是否属于归档范围、手续是否完备、内容是否真实有效。

7.2.1 归档材料必须是办理完毕的正式文件原件，确保档案的真实性和权威性。确实无法获得原件的，复印件上须加盖材料出具单位的红色公章，并注明“与原件一致”及日期，由经办人签字确认，方可归档。

7.2.2 材料必须对象明确、信息完整，凡针对个人的人事材料，必须清晰注明姓名、出生年月（公历、格式为 YYYYMM）、籍贯、身份证号等核心识别信息，确保材料与个人信息一一对应，杜绝错归、漏归。

7.3 完整性检查

每卷人事档案材料收集齐全率应达到 100%，确保档案材料完整无缺。对于缺少入党志愿书、连续六年考核表、转正定级表、学历学位证明等关键材料的，应立即建立《缺失材料追索台账》，明确追索责任、追索时限和具体措施，实行“挂账销号”管理，每月更新一次追索进度，直至材料补齐；确无法补齐的，应注明原因并由相关负责人签字确认，归档留存，确保档案信息可追溯。

8 整理与保管安全

8.1 分类与编码

人事档案分类应严格遵循国家统一的十大类分类法（履历材料，自传材料，考核鉴定，学历学位，政审，党团，奖励，处分，工资任免，其他），分类准确、层次清晰。每份材料右下角应用铅笔编写类号与顺序号，号体距右侧边沿 30mm、距下边沿 20mm，编写规范、清晰可辨，严禁涂改、乱编，确保档案整理有序、便于检索利用。

8.2 实物载体安全

8.2.1 装具：档案卷盒应采用无酸纸制作，PH 值控制在 7.0 至 8.5 之间，符合档案长期保存要求，防止纸张酸化老化。卷盒背脊标识应使用黑色耐水油墨打印，清晰标注档案编号、姓名、类别等核心信息，便于识别和管理。

8.2.2 保管状态：档案入库前必须进行专业消毒杀菌处理（如臭氧消毒，浓度不低于 20mg/m³，持

续 60 分钟），彻底清除病菌、虫卵等隐患，防止污染其他档案。对已破损、霉变、字迹模糊或虫蛀的档案，必须先进行专业托裱、修复或脱酸处理，经检验合格后方可入库，严禁未经处理的破损档案直接入库保管。

8.3 数字化副本安全

人事档案数字化工作严格依据 GB/T 33870-2017 执行，扫描分辨率不低于 300dpi，照片档案扫描分辨率不低于 600dpi，确保数字化副本清晰、完整，与原件一致。生成的图像文件应采用多级文件夹分类存储，命名规范、便于检索；每份数字档案应生成至少两个备份（在线热备+离线蓝光光盘备份），异地备份距离不小于 500 公里，建立备份管理台账，定期检查备份有效性，防范数字化档案丢失、损坏风险。

9 流转与交接安全

9.1 转递管理

人事档案转递是档案安全管理的关键环节，必须通过机要交通或指派专人送取，严禁个人自带、邮寄或通过普通快递转递，杜绝档案丢失、泄露风险。

9.1.1 包装：档案转递前，必须装入防水、防潮、防破损的专用档案袋，袋口贴密封条并加盖密封章，注明转递单位、接收单位、份数等信息，确保包装规范、密封完好。

9.1.2 交接确认：转出单位应在发出档案后 15 日内，通过机要渠道确认接收单位是否收到回执；若未收到回执，应立即启动催办程序，查明原因、及时处理。接收单位在收到档案后，应在 5 个工作日内核对档案数量、内容，确认无误后在回执上签字盖章并寄回转出单位，回执归档留存，实现转递全过程可追溯。

9.2 内部借阅

9.2.1 审批：查阅人事档案必须由查档单位出具正式介绍信，明确查档事由、人员名单及政治面貌，经档案所在单位分管领导签字批准后方可查阅。查阅过程中，必须有 2 名以上中共党员在场监督，严禁单人查阅，确保查阅过程规范、可控。

9.2.2 禁止行为：严禁在档案材料上涂改、划线、批注、折叠、抽页、增删，严禁私自复制、传播档案内容。借阅当场严禁使用个人电子设备拍照、录像，确需翻拍的，必须通过人事档案查阅专用翻拍设备，经权限密钥授权后操作，翻拍内容严格按规定用途使用，严禁私自留存。

10 数字化信息安全

10.1 网络隔离

承载人事档案信息的管理系统网络，必须依据 GB/T 22239-2019 通过网络安全等级保护三级及以上测评，严格落实网络安全防护要求。系统应实现与互联网物理隔离，采用网闸物理断开或单向导入技术，严禁接入外部网络，防范网络攻击、数据泄露等安全风险，保障数字化档案信息安全。

10.2 权限控制

采用细粒度的访问控制列表（ACL），严格落实权限分级管理要求，坚持“最小权限原则”，确保权限与岗位职责相匹配。

10.2.1 最小权限原则：普通员工的直系亲属无权查阅其详细人事档案；除组织人事部门专职管理人员外，其他部门人员仅能通过授权模块查阅与工作相关的部分公开信息（如职级、入职时间、岗位信息），严禁超权限查阅。

10.2.2 三员管理：严格落实系统管理员、安全保密管理员、安全审计员“三员分立”机制，明确各岗位权责，三员不得相互兼任、不得交叉履职，形成相互制约、相互监督的管控体系，防范权限滥用风险。

10.3 日志审计

人事档案数字化管理系统必须开启全面的操作日志功能，全面记录所有登录、查询、浏览、下载、打印、授权变更等操作行为，实现操作全过程可追溯、可审计。

10.3.1 日志内容：日志应包含事件发生的精确时间（UTC+8，精确至毫秒）、登录 IP 地址、MAC 地址、操作人、操作对象（如卷号、材料名称）、操作行为、操作结果等核心信息，确保日志信息完整、准确。

10.3.2 备份：日志数据保存时间不得少于 3 年，且必须进行异地备份，采用加密存储方式，防止日志被篡改、删除，为安全审计、责任追溯提供有力支撑。

11 利用与销毁安全

11.1 涉密档案管理

涉密人事档案（如因私出国审批、纪检审查、涉密岗位任职材料等）的密级确定，严格依照《中华人民共和国保守国家秘密法》《中华人民共和国保守国家秘密法实施条例》（2024 年修订）执行，明确密级、保密期限和知悉范围。查阅涉密人事档案，必须经本单位保密委员会审批，严格控制知悉范围，查阅过程全程监督，严禁私自复制、传播涉密内容，确保涉密档案安全。

11.2 销毁程序

对于超过保管期限（一般为死亡 5 年后）或失去保存价值的人事档案，应严格按照规定程序进行销毁，严禁擅自销毁、随意处置。

11.2.1 鉴定：由档案部门、业务部门及保密部门联合组成鉴定小组，按照国家档案鉴定标准，对拟销毁档案进行全面鉴定，提出销毁意见，编制《人事档案销毁清册》，明确销毁档案的名称、数量、编号、销毁原因等信息。

11.2.2 审批：《人事档案销毁清册》需经单位主要负责人签字批准，并报上级组织部门、档案主管部门备案，备案通过后方可实施销毁，严禁未经审批擅自销毁。

11.2.3 监销：销毁过程应由 2 名以上中共党员全程监销，采用符合保密要求的碎纸机（碎粒尺寸不大于 2mm×15mm）或化浆处理，确保档案彻底销毁、无法复原。监销人确认档案全部彻底销毁后，在《人事档案销毁清册》上签字确认，销毁记录、监销记录永久归档留存，实现销毁全过程可追溯。

12 外包服务管理

若将人事档案整理、数字化、保管等服务外包，应严格遵循 DA/T 68-2022 及国家保密相关规定，强化外包服务全流程管控，防范外包环节安全风险，确保人事档案安全。

12.1 资质审核

外包公司必须具备国家秘密载体印制（涉密档案数字化类）甲级或乙级资质，企业全员需通过无犯罪记录审查和保密培训，考核合格后方可参与外包服务；建立外包公司资质动态审核机制，定期核查资质有效性，对不符合要求的立即终止合作。

12.2 保密协议

与外包公司签订正式服务合同及《保密承诺书》，明确保密责任、保密期限和违约责任，设定违约金不低于项目总额的 50%，对因外包方原因造成档案泄露、篡改、丢失的，依法追究其法律责任和经济责任。

12.3 驻场管理

外包人员现场作业应在视频监控全覆盖、专人监督的环境下进行，严禁携带 U 盘、移动硬盘、具有蓝牙/WIFI 功能的电子设备进入作业区域。项目完成后，应彻底移除所有临时拷贝的数据，由第三方专业机构进行数据恢复检测，确保物理扇区数据不可恢复，同时收回所有涉密载体和操作权限，做好交接记录归档留存。

13 应急响应与灾难恢复

13.1 预案制定

各级各类组织必须结合实际，制定科学完善的《人事档案突发事件应急预案》，涵盖火灾、水灾、地震、台风等自然灾害，以及大规模数据泄露、系统宕机、档案损毁、盗窃等突发事件，明确应急组织机构、应急响应流程、处置措施和责任分工。应急预案每 24 个月至少组织一次实战化演练，通过以练促改、以改促优，提升应急处置能力，确保突发事件发生后能够快速响应、有效处置，最大限度减少档案损失。

13.2 灾难恢复指标

对于已数字化的人事档案管理系统，应明确灾难恢复目标，建立完善的灾难恢复体系，确保系统故障后快速恢复运行。

13.2.1 恢复时间目标（RTO）：核心档案查询、借阅等服务功能，应在系统故障发生后 4 小时内恢复，保障人事档案利用工作正常开展。

13.2.2 恢复点目标（RPO）：数据丢失量不得超过 60 分钟，通过定期备份、实时同步等技术手段，最大限度减少数据丢失，保障档案信息完整性。

13.3 灾备验证

每季度须对备份的人事档案数据（离线光盘、异地硬盘等）进行一次可恢复性抽检，抽检比例不低于备份总量的 5%，详细记录抽检过程、检测结果，填写《备份恢复验证记录表》归档留存。对抽检中发现的问题，立即整改，确保备份数据可正常恢复，筑牢灾难恢复防线，保障人事档案在极端情况下的安全。