机构编制实名制系统数据安全维护

王炳权
二连浩特市事业单位登记服务中心　内蒙古　二连浩特　011100

摘　要：本文围绕机构编制实名制系统数据安全维护展开研究，界定核心概念、梳理相关理论，分析系统数据安全的特殊性，剖析当前维护工作中的制度、技术、人员、监管等方面问题及根源，识别全生命周期数据安全风险并构建评估体系，最终提出“制度保障、技术防护、人员支撑、监管考核”四位一体的维护体系及优化措施，为提升系统数据安全防护水平、保障政务运行安全提供理论与实践支撑。

关键词：机构编制；实名制系统；数据安全维护

引言：机构编制实名制系统是规范编制管理、杜绝“吃空饷”的核心信息化平台，其数据涵盖机构、编制、人员等敏感信息，直接关系政务安全与公共利益。随着系统全覆盖推进和跨部门数据交互增多，数据泄露、篡改等安全风险凸显，当前维护工作存在诸多短板。基于此，本文聚焦系统数据安全维护，结合相关理论与实践现状，开展风险识别、评估及体系构建，助力筑牢数据安全防线，推动机构编制管理提质增效。

1 相关概念与理论基础

1.1 核心概念界定

（1）机构编制实名制系统：是机构编制管理的核心信息化平台，核心功能包括人员编制登记、信息核验、动态更新，数据构成涵盖机构信息、编制额度、人员档案等，其核心作用是实现编制管理规范化、精准化，杜绝“吃空饷”等问题。（2）数据安全维护：内涵是保障数据全生命周期安全，核心目标是防泄露、防篡改、防滥用，涵盖数据采集时的合规性审核、存储中的加密防护、传输中的安全管控，以及使用和销毁环节的规范流程。

1.2 相关理论支撑

（1）数据安全生命周期理论：作为全流程安全维护的逻辑框架，明确采集、存储、传输等各环节的安全管控重点，为系统数据安全维护提供系统性指导。（2）分级分类保护理论：根据数据涉密程度划分等级、分类管控，契合机构编制数据的涉密性特点，为敏感数据差异化防护提供理论依据。（3）风险管理理论：指导工作人员识别、评估系统数据安全风险，针对性制定防控措施，提升数据安全维护工作的有效性和针对性[1]。

1.3 机构编制实名制系统数据安全的特殊性

（1）数据敏感性高：涵盖机构设置、编制数量、人员信息等核心涉密数据，直接关系政务运行安全和公共利益。（2）数据关联性强：跨部门、跨层级数据交互频繁，安全维护需兼顾数据协同共享与独立防护的双重需求。（3）运维要求严格：需严格遵循政务数据安全相关法律法规，在保障数据安全的同时，兼顾业务办理效率，避免影响日常机构编制管理工作。

2 机构编制实名制系统数据安全维护现状及问题分析

2.1 机构编制实名制系统发展及数据安全维护现状

（1）系统发展现状：目前机构编制实名制系统已实现各级机关事业单位全覆盖，建设规模稳步扩大，核心数据涵盖机构职能、编制额度、人员信息、岗位配置等，运维模式以专人负责、分级管理为主，基本实现数据录入、核验、更新的信息化闭环管理，为机构编制管理提供了高效支撑。（2）安全维护现状：已初步建立数据安全维护相关制度，明确基础安全管理要求；技术层面部署了基础加密、防火墙等防护措施，规范数据访问权限；配备专职运维人员负责日常管控，开展定期数据备份、简单漏洞排查，基本保障系统正常运行和数据初步安全。

2.2 数据安全维护存在的主要问题

（1）制度体系不完善：缺乏统一的全流程数据安全维护规范，对数据采集、存储、传输等各环节管控标准不明确，各部门责任分工模糊，未形成闭环管理；数据安全应急预案针对性、可操作性不足，应对突发安全事件的能力薄弱。（2）技术防护有短板：数据加密技术应用不全面，敏感数据未实现分级加密保护；漏洞检测、入侵防御等技术手段滞后，缺乏智能化监测工具；数据备份恢复机制不完善，存在数据丢失、篡改的安全隐患。（3）人员素养待提升：部分运维人员数据安全意识薄弱，存在违规操作行为；专业技术能力不足，难以应对新型网络攻击和数据安全风险；缺乏常态化、系统化的安全培训，业务能力与维护需求不匹配[2]。（4）监管

机制不健全：缺乏常态化数据安全风险排查机制，对数据使用、共享环节的监管存在盲区；未建立科学的监督考核体系，对违规行为的惩戒力度不足，难以形成有效约束。

2.3 问题产生的根源分析

（1）思想认识层面：部分单位对机构编制数据安全的重要性认识不足，存在“重系统建设、轻安全维护”的倾向，将工作重点放在数据录入和业务办理上，忽视数据安全管控。（2）资源保障层面：数据安全维护的人力、物力、财力投入不足，技术升级换代滞后，难以适配新型安全风险；运维人员培训经费、培训资源短缺，导致人员专业能力提升缓慢。（3）管理机制层面：跨部门协同维护机制不健全，各部门各自为政，缺乏统一的统筹协调；未建立有效的考核约束机制，对数据安全维护工作的督促、考核不到位，难以调动相关人员的工作积极性。

3 机构编制实名制系统数据安全风险识别与评估

3.1 数据安全风险识别

（1）数据采集环节风险：数据采集缺乏统一规范，录入人员操作不严谨，易出现信息填写错误、格式不统一等问题；部分数据来源未经过严格核验，存在虚假数据、重复数据录入情况，不仅影响系统数据质量，还可能导致后续管理决策失误，埋下安全隐患。（2）数据存储环节风险：存储介质存在老化、损坏等问题，易造成数据丢失；核心敏感数据加密技术应用不到位，未实现分级加密存储，存在数据被非法访问、泄露和篡改的风险；部分存储设备运维不规范，缺乏定期检测和维护，进一步加剧存储安全风险。（3）数据传输环节风险：数据跨部门、跨层级传输时，部分传输通道未采取加密防护措施，或加密技术落后，数据易被网络黑客截获、窃取；传输过程中缺乏有效的数据校验机制，无法及时发现数据篡改、丢失等问题，影响数据传输的安全性和完整性[3]。（4）数据使用与销毁环节风险：数据访问权限管控不严格，存在越权访问、违规查询、复制数据等行为；部分工作人员违规使用数据，泄露核心涉密信息；数据销毁流程不规范，未采取专业的销毁手段，废弃存储介质中的数据易被恢复，造成数据泄露。

3.2 数据安全风险评估指标体系构建

（1）评估指标设计：围绕数据安全维护全流程，从制度、技术、人员、监管四个核心维度设计评估指标。制度维度涵盖维护规范、责任分工、应急预案等指标；技术维度包括加密防护、漏洞检测、备份恢复等指标；人员维度涉及安全意识、专业能力、培训情况等指标；监管维度包含风险排查、监督考核、违规惩戒等指标，确保指标科学可行、全面覆盖。（2）指标权重确定：采用层次分析法，结合机构编制实名制系统数据安全特点，邀请行业专家、运维人员进行打分，通过构建判断矩阵、一致性检验等步骤，明确各维度及具体指标的重要程度，合理分配权重，避免主观因素影响，确保风险评估结果客观、准确、可靠。

3.3 风险评估实施与结果分析

（1）评估实施：选取不同层级、不同类型的典型地区和机关事业单位，开展实地调研，通过查阅资料、现场核查、座谈访谈等方式，全面了解实名制系统运行及数据安全维护情况，对照构建的评估指标体系，对各风险点进行逐项打分、综合评估。（2）结果分析：根据评估得分，将数据安全风险划分为高、中、低三个等级，梳理各等级对应的风险点，明确高风险领域主要集中在敏感数据存储加密、越权访问管控等方面，中低风险主要体现在人员培训、流程规范等环节，为后续针对性制定风险防控措施明确重点领域和优先级。

4 机构编制实名制系统数据安全维护体系构建与优化措施

4.1 维护体系构建原则与总体框架

（1）构建原则：坚持合规性、系统性、实用性、前瞻性四大核心原则，严格遵循政务数据安全相关法律法规及行业标准，确保维护工作合法合规；立足系统运行全流程，统筹制度、技术、人员、监管等多方面要素，实现系统性防护；贴合机构编制管理实际需求，优化维护流程，兼顾数据安全与业务办理效率，避免形式化；预判网络安全发展趋势，融入先进防护技术，提升体系的可持续性和适配性，应对新型数据安全风险。（2）总体框架：构建“制度保障、技术防护、人员支撑、监管考核”四位一体的全方位数据安全维护体系。其中，制度保障是基础，明确维护工作的规范和准则；技术防护是核心，筑牢数据安全的技术屏障；人员支撑是关键，提升维护工作的执行能力；监管考核是保障，确保各项维护措施落地见效，四者相互衔接、协同发力，全面提升机构编制实名制系统数据安全防护水平[4]。

4.2 完善制度保障体系

（1）健全全流程维护制度：围绕数据全生命周期，制定覆盖数据采集、存储、传输、使用、销毁各环节的具体操作规范，明确各环节的操作标准、责任主体和管控要求。数据采集环节规范录入标准、核验流程，杜绝虚假、重复数据；存储环节明确加密要求、存储介质管理规范；传输环节规定加密方式、传输通道标准；使用

环节界定访问权限、操作范围；销毁环节明确销毁流程、技术手段，实现全流程有章可循、有据可查。（2）明确责任分工：建立“主管部门牵头、运维单位负责、使用单位协同”的三级责任体系，明确各主体职责边界。主管部门负责统筹规划、政策指导和监督协调；运维单位负责系统日常运维、技术防护和风险排查；使用单位负责本单位数据录入、使用的规范管理，落实专人负责数据安全，形成“谁主管、谁负责，谁使用、谁负责”的责任闭环，杜绝责任推诿。（3）完善应急预案：结合机构编制数据安全特点，制定针对性强、可操作性强的数据安全突发事件应急预案，明确应急组织架构、应急响应流程、处置措施和责任分工，涵盖数据泄露、篡改、丢失等各类突发情况。定期组织开展应急演练，检验应急预案的实用性和可操作性，提升工作人员应对突发安全事件的处置能力，最大限度降低安全事件造成的损失。

4.3 强化技术防护能力

（1）数据加密与脱敏：对机构编制核心敏感数据，采用AES高级加密算法进行全方位加密处理，实现存储、传输环节的加密防护；对非必要展示的敏感数据，实施数据脱敏与去标识化处理，隐藏身份证号、联系方式等核心信息，既保障数据安全，又不影响正常业务办理，防范数据泄露风险。（2）漏洞检测与修复：建立常态化漏洞扫描机制，定期采用专业扫描工具对系统进行全面漏洞检测，及时发现系统存在的安全隐患和漏洞。对检测出的漏洞分类分级管理，明确修复责任和时限，优先修复高风险漏洞；严格落实网络安全等级保护要求，定期开展等级保护测评，根据测评结果优化技术防护措施，筑牢系统安全防线[5]。（3）备份与恢复：建立“异地备份+定期备份”双重备份机制，明确备份频率、备份方式和存储位置，对核心数据实行每日增量备份、每周全量备份，确保数据可追溯、可恢复。定期对备份数据进行测试，检验备份数据的完整性和可用性，优化数据恢复流程，确保发生数据丢失、损坏等情况时，能够快速恢复数据，减少业务中断损失。

4.4 提升人员素养与监管水平

（1）加强人员培训：建立常态化培训机制，定期组织系统运维人员、使用人员开展数据安全培训，内容涵盖安全意识、法律法规、操作规范、专业技术等方面。邀请行业专家开展专题讲座，提升运维人员的漏洞检测、风险处置等专业能力，增强全体相关人员的安全意识，杜绝违规操作行为，筑牢人员安全防线。（2）健全监管机制：建立常态化风险排查机制，定期对系统运行、数据使用、技术防护等情况进行全面排查，建立风险台账，明确整改措施和时限；完善监督考核机制，将数据安全维护工作纳入相关单位和人员的绩效考核，细化考核指标，强化考核结果运用，对违规行为严肃追责问责，形成有效约束。同时，加强数据共享环节的安全管控，明确共享范围、权限和流程，防范共享过程中的数据安全风险。（3）完善协同机制：加强跨部门、跨层级协同配合，建立数据共享安全协议，明确各部门数据共享的安全责任和管控要求。搭建协同管控平台，实现数据安全信息互通、风险协同处置，打破部门壁垒，形成上下联动、左右协同的工作格局，提升数据安全维护的整体效能。

结束语

机构编制实名制系统数据安全维护是政务数据安全工作的重要组成部分，事关机构编制管理规范化、精准化推进。本文通过全面分析现状、识别风险、构建体系，提出针对性优化措施，有效弥补了当前维护工作的短板。未来需持续强化思想认识、加大资源投入，推动维护体系迭代升级，加强跨部门协同管控，常态化防范新型安全风险，为机构编制工作高质量发展提供坚实的数据安全保障。

参考文献

[1]毛先立,李莉,李攀.关于机构编制实名制信息化建设的实践与思考[J].行政科学论坛,2022,7(9):12-14.

[2]朱志强.基于实名制管理的机构编制档案管理信息化探索[J].黑龙江档案.2021,36(1):191-194.

[3]王宸.实施实名制管理,实现机构编制档案的信息化管理[J].现代经济信息,2023,21(7):104-106.

[4]韩东亚.如何让政府采购负面清单有章可循?[J].中国招标,2021,13(2):27-31.

[5]贾廷玉.以实名制管理，强化机构编制档案信息化管理[J].科技风,2022,6(2):75-78.