

SZSD

数 字 山 东 技 术 规 范

SZSD06 0012—2026

烟台市干部信息类党委数据综合管理技术 规范

Technical specification for comprehensive management of party committee cadre
information data in Yantai City

2026 - 08 - 19 发布

2026- 10 - 01 实施

烟台市大数据局 发 布

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。

本文件由中共烟台市委组织部提出，由烟台市大数据局归口。

本文件起草单位：中共烟台市委组织部、中共烟台市委办公室、烟台市大数据局、山东高速信息集团、烟台东方瑞创达电子科技有限公司。

本文件主要起草人：孙媛媛、李晓林、郭子陶、袁茂鑫、张德梅、刘刚、孙文杰、赵儒强、赵辉、孙德强、冯月姣。

烟台市干部信息类党委数据综合管理技术规范

1. 范围

本文件规定了党委数据干部信息综合管理中数据分类与存储、数据归集与交互、数据治理与分析、数据分析与利用、数据运维与安全等要求。

本文件适用于烟台市及所辖区（市）党委数据干部信息综合管理工作。涉密数据管理还应同时遵守国家保密法律法规及相关标准。

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 22239 信息安全技术 网络安全等级保护基本要求
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 36073 数据管理能力成熟度评估模型
GB/T 37973 信息安全技术 大数据安全管理指南
GB/T 37988 信息安全技术 数据安全能力成熟度模型
GB/T 38667 信息技术 大数据 数据分类指南
GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求
GB/T 14946.1—2025 全国组织、干部、人事管理信息 第1部分：数据元
GB/T 14946.2—2025 全国组织、干部、人事管理信息 第2部分：信息分类与代码
GB/T 25647—2010 电子政务术语
GB/T 33870—2017 干部人事档案数字化技术规范
GB/T 34960.5—2018 信息技术服务 治理 第5部分：数据治理规范
GB/T 43694—2024 数据安全技术 数据安全指南

3. 术语和定义

3.1.

干部信息 cadre information

反映干部个人基本情况、工作经历、政治表现、业务能力、考核评价、培训监督等方面的数据集

合。
[来源：GB/T 14946.1—2025，3.1，有修改]

3.2.

行政服务域 administrative service domain

面向党政机关和事业单位内部业务协同、数据共享与办公自动化的受控网络环境，与涉密网、互联网逻辑隔离。

非涉密数据 non-secret data

不涉及国家秘密，但可能包含工作秘密、内部管理信息或个人隐私的数据。涉密数据按国家保密法律法规管理。

3. 3.

内部数据 internal data

存储于涉密网或行政服务域中、仅限党委组织部门及授权单位内部使用的非公开数据，包括涉密类数据和内部非涉密数据。

3. 4.

外部数据 external data

来自互联网或外部单位、经脱敏或授权后可用于特定业务场景的非涉密数据，包括测评数据、互联网采集数据、外部共享数据等。

3. 5.

脱敏 desensitization

通过一定规则对敏感信息进行变形或屏蔽处理，防止隐私或敏感内容泄露。

3. 6.

最小够用原则 principle of minimum sufficiency

在满足业务需求的前提下，仅授予完成工作所必需的最少数据访问权限。

4. 综述

本规范遵循以下总体原则：

- a) 党管数据原则：坚持党对数据管理工作的全面领导，确保数据管理方向正确、标准统一，数据安全可控、使用合规，数据资源服务于党的组织建设和干部管理工作。
- b) 统一管理原则：建立“全市一个平台、一套标准、一个体系”的数据管理模式，统一数据分类、存储格式、交互协议、治理规则和安全策略，实现全市党委数据资源的一体化管理和高效利用。
- c) 依法依规管理原则：严格遵守《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国保守国家秘密法》等法律法规，以及中央组织部、国家保密局关于干部信息管理的专项规定，确保数据管理全流程合法合规。
- d) 全市一个数据平台原则：依托烟台市统一的干部人事编制一体化平台，实现市管干部、县管干部及其他人员数据的集中归集、统一治理、按需共享和智能应用，避免重复建设、多头采集。

5. 数据分类与存储

5.1 数据分类

5.1.1. 概述

按照数据性质（是否涉密）、使用范围（内部/外部）、管理要求（归集、共享、开放程度）三个维度划分为以下三类。

5.1.2. 涉密类数据

有关内容参照涉密信息系统相关管理规定执行。

5.1.3. 面向内部的非涉密数据

面向内部的非涉密数据是指不涉及国家秘密，但仅限于党委组织部门及授权单位内部使用，不得向社会公众公开的数据。包括但不限于：干部基础信息（姓名、性别、出生日期、身份证号等）、干部数字档案、干部业务数据（职务职级、考核结果、奖惩情况）、干部培训数据、干部监督数据（出境记录、重大事项报告等）、干部工资数据、干部研判数据、组织机构数据、党员数据、人才数据等。

此类数据统一存储在行政服务域，实行“按岗授权、最小够用”原则，仅限内部授权人员访问，禁止在互联网上存储、传输或发布。

5.1.4. 面向外部的非涉密数据

面向外部的非涉密数据是指经脱敏处理或依法可向社会公众、外部单位开放、共享的干部相关数据。包括但不限于：脱敏后的干部基本信息（姓名部分隐藏、年龄分段）、民主测评数据（汇总统计）、培训公开课程记录、干部任职公示信息、人才招聘信息、政策法规、办事指南等。

此类数据单独分区存储，与内部数据逻辑隔离，入库前必须完成脱敏、清洗、合法性校验。对外发布需经过保密审查和审批。

5.2. 数据存储

5.2.1. 涉密类数据存储

有关内容参照涉密信息系统相关管理规定执行。

5.2.2. 面向内部的非涉密数据存储

内部非涉密数据统一存储在行政服务域，采用国产信创数据库，主从复制 + 定期全量备份至独立存储节点，备份文件使用 SM4 加密。数据访问需记录日志（操作人、时间、类型、数据范围），保存不少于三年。导出需审批，文件加密并设置有效期。数据存储格式、目录结构、字段标准统一，满足内部业务协同与共享要求。

5.2.3. 面向外部的非涉密数据存储

外部非涉密数据（包括测评数据、互联网采集数据、外部单位共享数据）使用独立的数据库实例或独立表空间，应用层通过多数据源路由实现逻辑隔离。入库前完成脱敏、清洗、去重、合法性校验。脱敏规则：姓名保留首字、年龄分段、联系方式删除或替换为特定符号。对外数据接口通过统一网关管理，强制使用 HTTPS 和令牌认证，每次调用记录审计日志并生成数据指纹。外部数据定期（每月）进行内容审查，超范围公开或未经脱敏的数据立即下架。

6. 数据归集与交互

6.1. 数据归集

6.1.1. 归集原则

数据归集应遵循“统一标准、按职管理、源头唯一、及时准确、安全可控”五项基本原则。

6.1.2. 归集流程

数据归集流程明确发起方与完成方，形成“发起—校验—入库—确认”的闭环。

- a) 本人信息填报由干部本人或所在单位组织人事部门发起，填写后提交至所在单位审核，审核通过后完成归集。
- b) 业务系统自动归集由各业务系统（工资管理系统、干部任免系统、考核管理系统等）作为发起方，按照预设调度周期通过数据接口主动推送或由平台定时拉取，平台接收后进行格式校验、去重和逻辑检查，校验通过后写入主数据库，并将结果反馈给发起系统。
- c) 档案审核认定数据由档案审核部门在审核完成后发起，录入认定结论并上传扫描件等依据，经部门负责人复核后完成归集，同时通过消息队列向相关业务系统广播认定结果。
- d) 批量导入由数据管理员发起，上传标准化模板文件，系统执行逐行校验，全部通过后完成归集，部分失败时生成错误报告供下载修正。
- e) 所有归集操作均须记录日志，包含发起人、完成时间、数据来源、操作类型、归集状态等信息。

6.1.3. 归集方式

根据干部管理权限和数据类型，市管干部、县管干部、其他人员（包括科级以下干部、一般工作人员、党员、人才等）的数据归集可采用差异化的方式。数据类型分为三类：面向本人的基础信息（如健康状况、家庭成员及重要社会关系等）、面向业务的动态信息（如工资、职务职级、考核结果等）、需要组织认定的档案审核信息（如参加工作时间、出生日期、入党时间等）。

- a) 本人信息填报使用动态表单设计，表单模板存储在数据库，通过数据模型驱动前端渲染和校验；
- b) 业务系统归集使用分布式任务调度框架，数据接口采用超文本传输协议或 Web 服务规范，支持重试、降级、失败暂存队列；
- c) 档案审核认定数据：审核完成后，通过消息队列发送“认定完成”事件，消费者服务将认定数据写入主数据库，并同步写入全文搜索引擎用于检索；
- d) 批量导入功能支持电子表格模板，导入时进行逐行校验，错误数据生成错误报告并提供下载；
- e) 其他人员的数据归集周期可根据管理需要灵活设置，如通过统计数据、人才集团数据、在外人才库归集等方式，一般每半年或一年集中采集一次。

6.2. 交互方式

6.2.1. 数据范围

内部数据，是指存储于涉密网或行政服务域中、用于党委组织部门内部业务协同与干部管理的非公开数据，具体包括：涉密网内的涉密类干部数据（按国家保密法规管理）；行政服务域内的市管干部、县管干部及其他人员的干部基础信息、数字档案、业务数据（如职务职级、考核结果、工资信息、培训记录）、监督数据、研判数据、组织机构数据、党员数据、人才数据等。内部数据仅限内部授权人员按“最小够用”原则访问，不得在互联网上存储或传输。

外部数据，是指来自互联网或外部单位、经脱敏或授权后可用于特定业务场景的非涉密数据，具体包括：测评数据（如民主测评、在线考试等）、互联网公开采集数据（如干部公开履历、媒体报道等）、外部单位共享数据（如公安身份核验、编制信息、社保医保数据等）。外部数据需单独分区存储，与内部数据逻辑隔离，入库前必须完成脱敏、清洗和合法性校验，仅向授权业务场景开放使用，不得直接落地或逆向还原个人隐私信息。

6.2.2. 内部数据交互

涉密网、行政服务域、互联网三个网络区域之间存在严格的网络安全边界。涉密网交互有关内容，参照涉密信息系统相关管理规定执行。行政服务域与互联网之间通过前置机进行受控交互。所有跨区域数据交换需经过审批、审计和内容检查。

6.2.3. 外部数据交互

可利用多网络部署技术优势，构建涉密网、行政服务域、公共服务域等交互中心，与有关部门共同制定统一接入标准，接入过程中，严格规范数据格式、保障数据质量，明确干部数据与相关业务数据的核心关联字段，确立科学的数据关联标准，明确合理的数据引入频率，落实严格的引入安全管控要求，遵循规范的治理流程，建立健全异常数据识别、核查、整改、验收的异常处理机制，全面提升干部数据的真实性、完整性和规范性。

当外部数据与内部数据或不同外部数据源之间出现不一致时，应按照以下标准进行处理：

- a) 不一致检测：系统每日自动执行数据比对任务，对比范围包括但不限于：外部公安数据（身份证号、姓名）与内部干部信息；编制数据（在编状态）与内部在岗信息；工资数据（职务职级对应待遇）与内部任免信息；社保、医保数据与内部人员状态信息。比对任务通过数据质量管控平台执行，发现不一致时自动生成差异记录，包含差异字段、双方数据值、数据来源、比对时间、差异类型（如值不同、一方缺失、格式不符等）。
- b) 差异分级：根据不一致对业务的影响程度，分为三个等级：
 - 1) I级（严重）：影响干部身份认定、任免决策或待遇核定的不一致，如身份证号不符、在编状态冲突、职务职级与工资待遇严重不匹配等。
 - 2) II级（一般）：影响日常管理但不会造成重大后果的不一致，如联系电话、家庭住址、学历信息等。
 - 3) III级（轻微）：仅用于统计分析或辅助参考的不一致，如培训学时统计差异、考核评语表述不同等。
- c) 处理流程：
 - 1) 发现差异后，系统自动将差异记录推送至数据责任单位（内部数据以市委组织部干部信息管理机构为主，外部数据以提供方为主）；
 - 2) 责任单位在2个工作日内（I级）、5个工作日内（II级）、10个工作日内（III级）完成核查；
 - 3) 核查确认内部数据有误的，由内部责任单位依据原始依据进行修正，修正后重新比对直至一致；
 - 4) 核查确认外部数据有误的，由技术支持单位联系外部数据提供方，提交数据纠错申请，待外部系统修正后重新获取并比对；
 - 5) 对于因时间差导致的合理不一致（如刚办理退休但社保尚未同步），应建立白名单机制，标注“待同步”状态并设置自动重试周期（如72小时内每日重试）。

6.2.4. 业务协同交互

业务设计需涵盖人员“进、管、出”全环节，比如，用编进人计划业务、增人业务、减人业务、日常业务等，实现人员日常管理精细化、规范化。

各类业务均需经一体化平台严格审核审批，审批通过后，平台与社保、医保、财政、公积金等外部系统实现业务协同、数据共享，同步相关业务数据至各外部系统，由各系统完成对应业务办理。

各外部系统办结业务后，需将办理结果反向同步至一体化平台，平台汇总各类办理结果，针对减人

业务生成办结凭证，同步至发起业务单位，完成人员“出”环节闭环管理，同时实时更新平台编制数据库，及时释放对应编制额度，保障编制资源合理利用。

所有业务办理需严格遵循本规范，确保流程合规、数据准确、协同顺畅，提升人员管理及业务办理效率。

6.2.5. 技术要求

行政服务域与互联网交互：使用前置机部署网关，所有请求经过应用防火墙，数据通过加密隧道传输。

婚姻数据、医保数据交互：基于数据集成管道构建，使用通用序列化格式，消息队列作为数据总线，保证高吞吐和顺序性。

数据比对流程：使用批量计算框架，对比国家与省内婚姻数据差异，差异数据写入异常库，通过任务调度生成整改工单。

业务协同交互：一体化平台通过开放接口对外提供服务，外部系统调用接口时需携带签名的请求头（时间戳+随机数+签名），防止重放攻击。减人业务闭环通过消息队列异步通知并等待回执，超时自动重试。

7. 数据治理

7.1. 数据治理框架

需要建立“事前预防、事中控制、事后改进”的全链条治理流程，形成“事前预防（字段级校验）、事中控制（记录/跨表级校核）、事后改进（问题闭环）”的全链条治理流程。

数据治理对象需要覆盖干部基本信息、工作经历、家庭成员、简历、考核谈话、工资、职务职级等核心数据项。

7.2. 数据治理要求

完整性：核心数据项（姓名、身份证号、任免时间、考核结果等）不可为空；非核心数据项缺失率不超过 5%。

准确性：与公安、编制、工资等权威数据源交叉比对，一致率不低于 99%。字段间逻辑关系（如出生日期与身份证号）一致率达 100%。

一致性：同一数据在不同业务系统（如基本信息表与工资表）中保持一致，跨表一致率不低于 98%。

及时性：数据变更后应在 24 小时内完成归集更新；校核发现问题应在 7 个工作日内完成整改。

规范性：数据格式、编码、计量单位应符合 GB/T 14946 及本规范规定的标准。

7.3. 数据质量管控

7.3.1. 数据校核

需建立数据校核规则库，覆盖干部基本信息、工作经历、家庭成员、简历、考核谈话等核心数据项。每项规则应明确校核逻辑、触发条件、严重等级（错误/警告/提示）。

应支持字段级、记录级、跨表级三种校核粒度：

c) 字段级：检查格式、长度、取值范围、空值、特殊字符等。

d) 记录级：检查同一记录内字段间的逻辑一致性（如出生日期与身份证号不匹配、任职时间早于出生时间）。

- e) 跨表级：检查不同业务表之间同一数据的关联一致性（如干部基本信息表中的职务与工资系统中的职务等级应一致）。

需实现与外部数据源的交叉校核，包括与公安（身份证号、姓名）、编制系统（在编状态）、工资系统（职务职级对应待遇）等系统进行自动比对。

数据校核应以周期性（每日、每周、每月）和事件触发（数据导入、修改、归集后）两种方式执行。

校核结果需生成结构化报告，包含校核时间、规则名称、问题数据记录、问题描述、严重等级、建议处理方式。报告应支持导出和按权限查阅。

对于发现的问题数据，应建立闭环处理流程：问题登记 → 责任部门确认 → 数据修正 → 复核验证 → 关闭。所有操作步骤需记录在案，可追溯。

校核规则库应支持动态扩展，允许业务人员通过规则配置界面新增、修改、启用/停用规则，无需修改代码。

7.3.2. 业务质量管控

所有信息录入界面（包括基本信息、工作经历、家庭成员、简历、考核谈话等）需在字段层级实施实时校验。校验内容包括但不限于：字段长度、数据格式（如日期、身份证号、电话号码）、数值范围、必填项、特殊字符过滤。

表单提交前，系统需再次执行完整的数据校验，确保所有字段通过规则后才能提交。不符合要求的字段应高亮显示并给出具体错误提示。

表单填写完成并提交后，系统应自动触发数据校核任务。校核范围包括字段间逻辑一致性（如出生日期与身份证号不符、任职时间早于出生时间）以及跨业务表的关联一致性（如基本信息中的职务与工资系统中的职务等级匹配）。

校核完成后，系统需通过站内消息等方式向录入人员发送校核结果通知。通知内容应包含：校核通过/失败状态、问题数量、问题概要描述。

对于校核发现的问题数据，系统应支持录入人员在线查看详细问题列表，并允许在原表单基础上进行修正。修正后应支持重新发起校核。

所有业务表单的校验规则与校核规则需统一管理，并支持业务人员在不修改代码的情况下进行配置调整。

校验与校核的操作日志（包括时间、操作人、表单类型、校验结果、校核结果）需完整记录，保存期限不少于三年。

7.3.3. 技术要求

校核规则库存储于关系数据表，规则表达式使用表达式引擎动态解析。

字段级校核：前端使用表单校验，后端使用参数校验框架双重校验。

记录级与跨表级校核：编写批量处理任务，每日凌晨扫描全量数据，生成结果集并比对，结果写入校核结果表。

与外部系统交叉校核：通过接口调用公安、编制、工资系统提供的比对服务，设置超时时间，失败时进入重试队列并告警。

校核报告导出为文档格式，通过任务调度定时发送至管理员邮箱。

闭环处理流程：问题数据生成后自动在运维平台创建工单，状态流转通过状态机管理，所有操作日志写入集中日志系统。

实时校验：使用组件内置校验规则，并结合自定义异步校验（如身份证号是否已存在）。

提交后完整校验：使用参数校验分组，并调用业务校验服务。

自动校核任务：通过消息监听机制在表单提交事件触发后异步执行校核，校核完成后通过实时通信

推送通知给前端。

校验规则配置：设计规则配置界面，支持非开发人员通过下拉框、条件组合配置校验逻辑，配置存储为通用数据格式，后端使用表达式引擎执行。

8. 干部信息数据标准

8.1. 干部基础数据

主要包含：基本信息、编制标识子集、教育学历、任职信息等 17 项信息集。

8.2. 干部数字档案

主要包含：审核报告单、用户权限、散材料目录、材料类别等 19 项信息集。

8.3. 干部业务数据

主要包含：职务职级、考核、奖惩等 25 项信息集。

8.4. 干部培训数据

主要包含：管理类别、职务层级、高端讲座、培训类型等 16 项信息集。

8.5. 干部监督数据

主要包含：出国境、重大事项、违法违纪等 18 项信息集。

8.6. 干部档案智能库房

主要包含：存储位置、转递信息、转出去向、机械臂控制、环境监控、执行方式等 32 项信息集。

8.7. 干部工资数据

主要包含：工资相关标识、基本工资推算过程、在职人员工资业务等 6 项信息集。

8.8. 干部研判数据

主要包含：信访举报、干部考察情况、熟悉领域、工作分工等 33 项信息集。

8.9. 组织机构数据

主要包含：机构基本信息、机构信访举报子集、单位年度考核情况、班子考察情况等 19 项信息集。

8.10. 党员数据

主要包含：组织关系信息、党内职务信息、“两代表一委员”信息、民主评议信息等 23 项信息集。

8.11. 人才数据

主要包含：所在地、现任职务、出生地等 9 项信息集。

9. 数据分析与利用

9.1. 基于大数据的全市干部数据分析

采用大数据技术整合干部基础信息、考核数据、培训记录、任职履历等结构化数据。通过 ETL 工具定期从各业务系统抽取数据，经清洗、转换后加载至分析型数据库。前端使用 BI 工具构建多维度分析看板，支持下钻、联动、筛选等交互操作。预警功能通过规则引擎配置阈值条件，定时任务触发比对应后生成预警消息并推送至消息中心。

9.1.1. 数据源头与加载内容

数据生成的首要环节是明确数据来源和采集内容。干部基础信息、任职履历、任免记录等核心数据来源于干部管理系统；年度考核结果、民主测评得分、考核评语等来源于考核管理系统和民主测评系统；培训记录来源于培训管理系统，包括培训班名称、时间、学时、类型及成绩；谈话记录和考察材料来源于考察谈话系统或电子档案；信访记录来源于信访管理系统或纪检系统。此外，工资信息从工资管理系统获取，编制状态从编制管理系统获取。上述数据涵盖干部基本信息、工作经历、家庭成员、简历、考核谈话等主要业务范围，是后续分析和研判的基础原材料。

9.1.2. 数据采集与加载方式

数据采集根据源头系统的特点和网络环境，采用多种方式组合进行。对于初次建库或需要定期全量同步的场景，采用全量抽取方式，将源头系统的全部历史数据一次性加载到分析平台。对于日常变更的数据，采用增量捕获方式，通过监听业务数据库的变更日志，实时或定时获取新增、修改和删除操作。对于跨部门、跨网络的数据交换，采用接口调用方式，外部系统通过加密的数据接口进行推送或拉取。对于离线数据或历史档案，采用文件导入方式，从电子表格、文本文件等格式中解析数据，并在导入过程中完成加密校验和格式检查。

9.1.3. 调度与执行周期

数据生成过程按照预设的调度周期自动执行，确保分析数据的及时性和准确性。增量同步任务每 15 分钟或每小时执行一次，实时捕获各业务系统的数据变更。全量同步任务每日凌晨执行，同步前一日变更量较大的数据表，保证数据的完整一致性。跨系统交叉校核任务每周一凌晨执行，例如与公安、编制、工资等外部系统进行数据比对，发现不一致问题。特征工程计算任务每日凌晨执行，基于原始数据计算干部成长路径特征、能力素质曲线、人岗匹配度等衍生指标。预警规则扫描任务每日早晚各执行一次，扫描预警指标库中的各项条件，发现触发规则的情形后生成预警消息。数据质量校核任务每日凌晨执行，并结合数据入库事件触发，对数据进行多层级校验并生成质量报告。

9.1.4. 数据处理流程

数据从源头系统到最终分析应用，经过多个处理环节形成完整的数据流。首先，数据采集模块从各业务系统抽取数据，存放于原始数据层，保留数据的原始状态。其次，数据清洗模块对原始数据进行去重、空值填充、格式标准化、字段映射和敏感信息，消除数据中的噪声和不一致问题。然后，数据转换模块按照分析模型的要求进行数据聚合，计算年龄分段、任职年限分段等衍生字段，将数据转换为适合分析的格式。接着，转换后的数据加载到分析型数据库中，供查询和分析使用。上述各个环节通过自动化任务调度系统进行编排，定义任务之间的依赖关系和执行顺序，并支持失败自动重试。同时，运行监控模块持续跟踪数据同步延迟、任务失败率、数据量波动等关键指标，发现异常时及时告警。

9.1.5. 技术实现要求

数据仓库应采用分层架构，包括原始数据层、清洗层、汇总层和应用层，各层之间数据流转通过自动化任务完成。

数据采集应同时支持批量抽取和实时捕获两种模式，批量抽取用于全量初始化，实时捕获用于日常变更同步。

数据清洗与转换应采用可配置的规则引擎，支持字段映射、格式标准化、空值处理、异常数据过滤等功能。

分析型数据库应支持高并发查询和多维聚合分析，能够满足多维度下钻、联动筛选等交互操作需求。

前端分析看板应提供图表可视化展示，支持按时间、组织层级、干部类型等多维度的动态筛选和对比分析。

预警功能应采用规则引擎配置阈值条件，通过定时任务触发比对，生成预警消息后统一推送至业务部门。

9.2. 基于大模型的干部班子智能研判

采用预训练大语言模型作为基础能力层，结合本市干部数据进行微调（Fine-tuning）。将干部档案、考核评语、谈话记录等非结构化文本转化为向量嵌入，构建干部知识库。班子评估通过图神经网络提取班子内部成员关系特征，结合多维属性进行整体评分。胜任力推演采用对比学习框架，基于历史提拔案例训练匹配模型。推荐结果通过注意力机制输出关键决策因子。以 API 形式提供研判服务。

利用大模型技术对领导班子整体配置进行量化评估，评估维度包括年龄结构、专业分布、任职来源、性格特质互补性等。

应建立干部胜任力推演模型，基于干部历史表现数据与目标岗位要求，输出胜任概率及关键影响因素。

应具备后备干部智能筛选功能，根据岗位需求特征自动匹配干部库中符合条件的人选，并按匹配度排序，同时输出匹配依据。

应支持班子调整方案的模拟对比，对不同组合方案在平均年龄、专业结构、协作风险等指标上进行量化比较。

应具备生成个性化考察谈话提示功能，依据干部数据特征（如任期未完成任务、信访记录等）自动列出需重点核实的访谈要点。

技术要求如下：

大语言模型基座选用可私有化部署的模型，使用微调技术，训练数据为脱敏后的干部考核评语、谈话记录。

向量化：使用文本向量化模型将文本转为向量，存储于向量数据库。

图神经网络：使用图深度学习框架构建班子内干部关系图（共事关系、上下级关系等），通过图卷积网络计算班子整体协调性评分。

胜任力推演：基于梯度提升树等算法训练分类模型，特征包括任职年限、考核结果、培训完成度等，输出胜任概率及特征贡献解释值。

后端提供推理服务，业务系统通过远程调用接口调用，结果缓存至内存缓存。

前端展示使用关系图库，支持班子方案模拟对比（拖拽替换成员实时计算指标）。

9.3. 基于物联网的智能档案库房

采用超高频 RFID 技术，每份档案粘贴无源抗金属标签。库房内安装固定式读写器（每层货架部署天线）和手持式盘点终端。定位算法采用 RSSI 信号强度与相位差结合的多点定位，实现亚米级位置标定。出入口设置门禁式读写器与红外传感器，自动记录档案进出并触发声光提示。环境传感器通过 LoRa 或 Zigbee 组网，数据汇聚至物联网网关，与库房动环监控系统联动。全生命周期事件写入区块链存证，确保不可篡改。

每份纸质档案需加装物联网电子标签，库房内应部署定位感应设备，实现档案所在货架层及具体位

置的实时查询与地图标定。

需实现档案出入库自动感应记录，自动采集操作人、操作时间、档案编号，形成电子借阅台账，并支持超期未归还自动提醒。

库房内应部署温度、湿度、烟雾、水浸、光照传感器，实时监测环境参数，超出设定阈值时自动告警并可联动空调、除湿机等调控设备。

需支持自动盘点功能，系统通过感应扫描比对台账，自动识别档案错位、缺失或未归还情况，生成盘点报告。

应在库房出入口及通道部署门禁与移动感应装置，非授权时段或人员进入时自动记录并发出告警。

需实现档案全生命周期事件自动记录，包括接收、入库、上架、借阅、归还、复制、销毁等环节，记录不可篡改且可追溯。

技术要求：

射频识别读写器：采用工业级读写器，通过物联网协议上报标签信息。

后端定位服务：使用物联网消息接收组件接收数据，定位算法采用改进型参考标签定位法，定位精度优于 0.5 米。

环境传感器：使用低功耗无线组网技术，网关汇聚数据，数据上报至时序数据库。

盘点任务：定时触发射频识别读写器轮询，系统比对预期位置与实际位置，差异生成报表，支持手持终端离线盘点。

门禁联动：出入口读写器检测到未登记档案进出时，调用摄像头抓拍并保存，同时触发声光报警器。

10. 数据运维与安全

10.1. 数据运维管理

10.1.1. 运维目标

需建立统一、规范、高效的数据运维体系，保障党委干部信息综合管理平台及各业务系统的稳定运行，确保数据的完整性、可用性、安全性和可追溯性，支撑干部信息全生命周期的闭环管理。

10.1.2. 运维范围

数据运维涵盖以下内容：

数据基础设施运维：服务器、存储设备、网络设备、安全设备、物联网感知设备（RFID 读写器、环境传感器等）。

数据平台运维：数据库系统、数据交换平台、消息队列、全文检索引擎、向量数据库等。

业务应用运维：干部综合管理平台、档案管理系统、数据校核系统、大模型推理服务、BI 分析看板等。

数据资产运维：数据归集、清洗、校核、备份、恢复、归档、销毁等数据全生命周期操作。

安全运维：漏洞扫描、渗透测试、日志审计、权限变更、应急响应等。

10.1.3. 运维责任主体

市委组织部干部信息管理机构是数据运维的业务主管单位，负责提出运维需求、审批运维操作、监督运维质量。

市大数据局或指定技术支持单位是数据运维的技术实施单位，负责系统部署、日常监控、故障处理、数据备份、性能优化等具体工作。

各业务系统使用单位（各区市党委组织部、市直单位组织人事部门）负责本单位职责范围内的数据录入、校核确认、问题反馈等操作。

运维外包人员需签订保密协议，并通过安全背景审查，操作权限按最小够用原则授予，所有操作纳入审计。

10.1.4. 运维依据规范

数据运维工作应遵循以下依据：

法律法规：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《商用密码管理条例》；

国家标准：GB/T 22239（等保基本要求）、GB/T 28827（信息技术服务 运行维护）系列标准、GB/T 36073（数据管理能力成熟度评估模型）；

行业规范：中央组织部关于干部信息管理的相关技术规范、山东省大数据发展促进条例、数字山东建设总体规划；

本规范各章节关于数据分类、存储、归集、交互、治理、分析的技术要求。

10.1.5. 运维台账

建立统一电子化运维台账：

记录内容：系统启停、数据备份与恢复、用户权限变更、故障处理、软件升级、硬件更换、安全事件等；

每条记录包含操作人、操作时间、操作内容、操作原因、审批人信息；

台账设置只读权限，保存期限不少于三年，重大安全事件记录永久保存；

每月抽查审核，问题追溯通过台账快速定位。

10.1.6. 运维操作规范

所有变更操作（配置修改、数据批量处理、权限调整）需提前制定方案，经业务主管和技术负责人双重审批后方可执行。

生产环境操作应在非业务高峰期进行，并在测试环境中完成验证。

数据批量导出、删除等敏感操作需双人复核，操作过程全程录屏或日志记录。

运维操作应保留回滚方案，确保异常时可快速恢复。

10.2. 数据安全保障

10.2.1. 软件安全

用于干部、党员、人才信息管理的软件系统，需设置分级操作权限。不同岗位的人员只能访问其工作职责范围内的数据，例如录入人员不能查看考核结论，审核人员不能修改原始信息。

系统应自动记录每一次关键操作，包括谁、什么时间、对哪条数据做了什么操作（如新增、修改、删除、导出）。这些操作记录应当长期保存，便于事后追溯，鼓励对数据库进行专项技术加密、防控、审计。

任何系统功能的新增、修改或升级，需先在隔离的测试环境中验证，确认不影响现有数据安全与业务正常运行后，再经过审批正式上线。

系统应具备异常行为报警功能，例如非工作时间大量导出数据、短时间内频繁查询不同干部信息等，系统能自动向管理员发出提醒。

对于不再使用的系统账号，需在人员调岗或离职后 24 小时内完成注销或禁用。

涉及生成式人工智能的软件模块（如大模型研判服务），应遵守《生成式人工智能服务管理暂行办法》，对训练数据进行脱敏处理，生成内容需标注来源，建立人工复核机制。

10.2.2. 硬件安全

承载干部数据的服务器、存储设备、网络设备等硬件，需放置在专用机房或安全可控的机柜中，机房门禁采用双重验证（如刷卡加密码），进出有记录。

机房环境应配备温度湿度控制设备，确保设备在适宜环境中运行。同时配备不间断电源和备用发电机，防止突发断电导致数据损坏或业务中断。

重要硬件设备应建立巡检制度，每月至少进行一次全面检查，包括设备运行状态、硬盘指示灯、散热风扇、连接线缆等，发现问题及时处理并记录。

对即将报废或更换的硬盘、存储介质，需采用不可恢复的物理销毁或专业消磁方式处理，严禁直接丢弃或转作他用。

关键设备（如主数据库服务器）应配置热备或冷备机制，当主设备发生故障时，备份设备能快速接管，保证业务不中断。

10.2.3. 网络安全

所有数据在网络传输时需采用加密方式（如 TLS/SSL、国密算法）。严格区分内部工作网络与互联网，敏感数据严禁在互联网上传输或存储。内部网络与外部网络之间的数据交换需通过安全隔离设备进行单向或审批后传输。

严格区分内部工作网络与互联网。涉及干部个人信息、考核结论、家庭情况等敏感数据，严禁在互联网上传输或存储。内部网络与外部网络之间的数据交换，需通过安全隔离设备进行单向或审批后传输。

对连接内部网络的计算机和设备实行准入管理，未经授权的设备不得接入。外来笔记本电脑或移动设备如需接入，需经过安全检查和审批。

对连接内部网络的计算机和设备实行准入管理。定期（至少每半年一次）进行安全漏洞扫描和渗透测试。用户密码需符合复杂度要求并定期更换。

同时，网络安全管理应满足 GB/T 22239 相应等级保护要求，每年开展等保测评。涉及跨网数据交换的，应符合 GB/T 39477（政务信息共享数据安全技术要求）。

定期（至少每半年一次）对内部网络进行安全漏洞扫描和渗透测试，发现弱口令、未关闭的高危端口、异常网络连接等问题，需在规定时间内整改。

所有用户需使用符合复杂度要求的密码（长度不少于 8 位，包含字母、数字、特殊符号），并每三个月更换一次。禁止将密码写在便签上或告知他人，系统应支持首次登录强制修改初始密码。

参 考 文 献

- [1] GB/T 36073-2025 数据管理能力成熟度评估模型
 - [2] GB/T 36344-2018 信息技术 数据质量评价指标
 - [3] GB/T 37722-2019 信息技术 大数据存储与处理系统功能要求
 - [4] GB/T 38667-2020 信息技术 大数据 数据分类指南
 - [5] GB/T 45288.1-2025 人工智能 大模型 第 1 部分：通用要求
-