ICS 35.240.99
CCS L 67

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX-XXXX

变电二次系统用数字档案资料管理技术要求

Technical requirements for digital archives management of substation secondary systems

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国商业企业管理协会　　发 布

目　　次

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。

本文件由国网湖北省电力有限公司宜昌供电公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：国网湖北省电力有限公司宜昌供电公司、常州明睿电力科技有限公司、武汉市豪迈电力自动化技术有限责任公司、国网湖北省电力有限公司技术培训中心、南方电网广州供电局变电管理三所。

本文件主要起草人：陈泽华、倪呈祥、张洋、官习炳、龚康、陈俊杰、叶涛、刘勤、夏昊锴、石旭刚、徐威、尹明、李敬东、刘红霞、朱长东、艾洪涛、罗鹏、刘俊、程金牛、聂道琦、汪谦、杨彬、吴鹏、刘念、邓金华、施微、黄昱皓、张思奇、冯云斌、黄禹、鲜万春、裴磊、孙培文、鲍易辉、范俊、周昊东、郭仕林、李渊、李紫嫣、张蝶、周美娣、耿梦媛、王平、邵铭少。

变电二次系统用数字档案资料管理技术要求

1 范围

本文件规定了变电二次系统数字档案资料管理的术语和定义、总体要求、数据管理、管理流程、质量要求、系统要求、安全管理及系统运维管理的要求。

本文件适用于电力企业对变电二次系统产生和管理的数字档案资料进行全生命周期管理。

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 33190 电子文件存储与交换格式 版式文档

GB/T 39784-2021 电子档案管理系统通用功能要求

DL/T 587-2016 继电保护和安全自动装置运行管理规程

GB/T 14285-2023 继电保护和安全自动装置技术规程

Q/GDW 1914-2013 继电保护及安全自动装置验收规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

变电二次系统 substation secondary systems

由测量、控制、保护、信号、通信等设备及相关回路构成，用于监视、控制、保护和调节变电一次系统运行的电气系统。

3.2

数字档案资料 digital archives

以数字形式记录和存储的，与变电二次系统相关的设备参数、运行记录、检修报告、图纸、说明书、规程等各类信息资料。

3.3

全生命周期管理 life cycle management

对数字档案资料从产生、收集、整理、存储、利用到销毁的全过程进行管理和控制。

3.4

访匹值 access matching Value

过对访问人员的部门、职位、职级、参与项目类型、次数及负责程度等职责状态信息进行量化赋值处理得到的数值，用于匹配访问人员的权限范围类型等级。

3.5

异常数字档案文件 abnormal digital archive files

通过获取当前监测时段内数字档案文件的被点击次数、运载速率和访问时长，经归一化处理得到访问状态评估值，当该评估值大于或等于访问状态评估阈值时，标记为异常数字档案文件。

3.6

访限人数 access limit number

根据异常数字档案文件的访限值与云数据库中访限状态判定表对照匹配，得到访限状态等级所对应的允许访问该文件的人数。

3.7

目标访问人员 target authorized personnel

对位于允许访问异常数字档案文件地理位置范围内的可选访问人员，根据其点击时值、历访值和第二权范值计算优选值，按优选值降序排列后，选取与访限人数相匹配的人员。

3.8

综合访倾值 comprehensive access tendency value

通过对访问人员的访行倾值（基于回访次数、停留时长和深击次数计算）和访需倾值（基于倾向目标词的访问时长和点击次数计算）进行归一化处理得到的数值，用于确定是否进行数字档案文件个性化推送。

4 总体要求

4.1 完整性

数字档案资料管理系统应确保变电二次系统全生命周期内相关档案资料的完整性收集、存储和管理，包括但不限于设计阶段的图纸、说明书，施工阶段的记录、调试报告，运行维护阶段的设备缺陷记录、检修报告等。

4.2 准确性

系统中存储的数字档案资料应准确反映变电二次系统的实际情况，数据录入、修改等操作应经过严格审核，保证档案资料内容、数据的准确性。

4.3 可用性

数字档案资料应易于检索、查询和利用，系统应提供便捷的用户界面和高效的检索工具，满足不同用户在不同场景下对档案资料的使用需求。

4.4 安全性

应建立安全管理体系，保障数字档案资料的安全存储、传输和使用，防止数据泄露、篡改和丢失。

4.5 可追溯性

应建立档案管理记录，能够追溯数字档案资料的来源、修改历史和使用情况，便于责任认定和问题排查。

5 数据管理

5.1 数据分类与编码

5.1.1 根据变电二次系统的特点，对数字档案资料进行合理分类，如设计资料类、施工资料类、运行维护资料类、设备管理资料类等。具体要求如下：

a) 设计资料类应包含符合 GB/T 14285-2023 要求的继电保护及安全自动装置设计图纸、技术参数说明等；
b) 施工资料类应包含依据 Q/GDW 1914-2013 形成的安装调试记录、验收报告等。
c) 运行维护资料类应包含遵循 DL/T 587-2016 生成的设备运行日志、定值调整记录等。

5.1.2 制定统一的档案资料编码规则，编码应具有唯一性、稳定性和可扩展性，便于档案资料的识别、检索和管理。例如，可采用层次码结构，前几位表示档案类别，中间几位表示变电站名称、电压等级等信息，后几位表示具体档案资料的流水号。

5.2 元数据管理

5.2.1 定义适用于变电二次系统数字档案资料的元数据元素集，包括但不限于档案名称、文件编号、形成时间、作者、所属项目、关键词、文件格式、密级等。

5.2.2 元数据应与数字档案资料关联存储，在档案资料的录入、修改、迁移等过程中，确保元数据的同步更新和准确维护。

5.2.3 变电二次系统数字档案资料的元数据应符合 GB/T 39784-2021 中表 34 的规定。

5.3 数据录入与更新

5.3.1 应提供多种数据录入方式，如手工录入、批量导入、系统接口对接自动采集等，满足不同来源数据的录入需求。录入界面应设计友好，提供必要的提示和校验功能，确保数据录入的准确性。

5.3.2 应建立数据更新机制，当变电二次系统发生设备变更、技术改造、运行维护情况变化等时，能够及时更新相应的数字档案资料，保证档案资料与实际情况的一致性。更新操作应记录详细的日志，包括更新时间、更新人、更新内容等。

5.4 数据存储

5.4.1 选择可靠的存储介质和存储架构，确保数字档案资料的长期安全存储。可采用磁盘阵列、网络存储设备等，并建立冗余备份机制，防止因存储设备故障导致数据丢失。

5.4.2 根据数字档案资料的重要性和使用频率，采用分级存储策略，将常用、重要的数据存储在高性能存储设备上，以提高访问速度；将不常用的数据存储在低成本、大容量的存储设备上。

5.4.3 对存储的数字档案资料进行定期的完整性和可用性检查，及时发现并修复数据损坏、丢失等问题。

5.4.4 数字档案资料存储要求应符合 GB/T 33190 的规定。

6 管理流程

6.1 收集

6.1.1 应明确数字档案资料收集范围，包括但不限于设备出厂参数、安装调试记录、日常运行数据、检修维护报告、故障处理记录等。

6.1.2 制定收集计划，规定各类资料的收集时间、收集方式和责任部门及责任人员。对于实时产生的运行数据，采用自动化采集技术；对于其他资料，通过相关业务部门定期提交或系统接口自动获取。

6.2 整理

6.2.1　按照资料类型、时间顺序、设备类别等进行分类，建立清晰的分类体系。例如，可分为设备资料类、运行资料类、检修资料类等。
6.2.2　对资料进行编号，确保每个档案资料都有唯一的标识，便于检索和管理。编号规则应具有科学性和可扩展性。
6.2.3　编写资料目录和元数据，详细描述资料的基本信息，如名称、创建时间、内容摘要、存储位置等，方便用户快速了解资料内容。

6.3　存储

6.3.1　选择合适的存储介质和存储设备，确保存储的稳定性和可靠性。优先采用大容量、高可靠性的磁盘阵列或云存储技术。
6.3.2　建立存储管理制度，定期对存储设备进行检查和维护，及时备份重要数据，防止数据丢失。备份数据应异地存储，确保在发生灾难时能够快速恢复。

6.4　利用

6.4.1　建立数字档案资料检索系统，提供多种检索方式，如关键词检索、分类检索、时间检索等，方便用户快速查找所需资料。
6.4.2　制定资料使用权限管理制度，根据用户角色和职责分配不同的使用权限，确保资料的合理使用和安全。例如，普通运维人员只能查看和下载相关运行记录，而管理人员可进行资料修改和删除操作。
6.4.3　开展数字档案资料的分析和挖掘工作，为变电二次系统的优化运行、设备维护和企业决策提供数据支持。例如，通过对设备运行数据的分析，预测设备故障，提前安排检修计划。

6.5　销毁

6.5.1　明确数字档案资料的销毁条件和期限，对于超过保存期限且无保存价值的资料，经相关部门审批后进行销毁。
6.5.2　采用安全可靠的销毁方式，确保销毁后的资料无法恢复。例如，对存储在电子介质上的资料进行多次覆盖擦除或物理销毁。

7　质量要求

7.1　内容质量

7.1.1　数字档案资料内容应完整、准确，涵盖所有必要的信息，数据记录应清晰、规范，符合相关技术标准和业务要求。
7.1.2　资料中的数据应具有一致性，不同来源的相关数据应相互印证，避免出现矛盾和冲突。

7.2　格式质量

7.2.1　数字档案资料应采用统一的格式存储，如 PDF、XML、JSON 等，便于数据的交换和共享。
7.2.2　资料的排版应规范、整齐，文字清晰，图表准确，符合文档格式要求。

8　系统要求

8.1　系统模块

8.1.1　硬件模块

数字档案资料管理系统硬件模块应包括：

d) 用户终端：供访问人员输入个人信息注册登录系统，接收服务器推送的可访问数字档案文件及相关通知；

e) 服务器：存储个人信息、权限范围类型等级、异常数字档案文件访限人数、目标访问人员及可推送数字档案文件等数据，协调各模块运行；

f) 云数据库：存储访限状态判定表、综合访倾状态判定表等数据，为系统分析处理提供数据支持。

8.1.2 软件模块

数字档案资料管理系统软件模块应包括：

a) 数据采集模块：采集访问人员的部门、职位、职级、参与项目类型、次数及负责程度等职责状态信息，发送至权限分配模块；

b) 权限分配模块：根据职责状态信息计算访匹值，匹配权限范围类型等级，并对应匹配可访问的数字档案文件范围；

c) 访问识别模块：监测数字档案文件的访问状态，分析处理得到异常数字档案文件及对应的访限人数，发送至访问排序模块；

d) 访问排序模块：根据访限人数及可选访问人员的优选值，选择目标访问人员；

e) 访问跟踪模块：监测访问人员的访问行为状态，分析处理得到可推送数字档案文件。

8.2 功能模块

数字档案资料管理系统的功能模块见表 1 。

表 1 数字档案资料管理系统功能模块及要求

功能模块	子功能
用户管理	访问人员个人信息注册、登录及信息维护
权限管理	职责状态信息采集、访匹值计算、权限范围类型等级匹配
档案访问管理	数字档案文件访问状态监测、异常识别与限制、访限人数确定
访问人员管理	位置信息获取、可选访问人员标定、优选值计算、目标访问人员选择
个性化推送管理	访问行为状态信息监测、访行倾值与访需倾值计算、综合访倾值分析、数字档案文件个性化推送
数据存储管理	个人信息、权限数据、访问状态数据、推送数据及各类判定表的存储与维护

8.3 功能要求

8.3.1 用户管理功能

8.3.1.1 应支持访问人员输入名字、身份证号、手机号等个人信息进行注册登录，确保身份准确追踪识别。

8.3.1.2 应提供个人信息查询与修改功能，保证信息的准确性和时效性。

8.3.2 权限管理功能

8.3.2.1 应能采集访问人员的部门、职位、职级等基础职责信息，以及参与项目类型、次数和负责程度等扩展信息。通过设定的权重系数计算第一权范值和第二权范值，经归一化处理得到访匹值，实现权限范围类型等级（一级、二级、三级）的自动匹配。权限范围匹配分析过程如下：

a) 获取访问人员的职责状态信息中的部门、职位和职级，并将部门、职位和职级进行赋值分析，得到访问人员的部门赋值、职位赋值和职级赋值，并分别标记为 bm、zw 和 zj，取其数值，得到第一权范值 dyz_1，计算公式如下：

$$dyz_1 = bm \times a_1 + zw \times a_2 + zj \times a_3 \quad \text{.....(1)}$$

式（1）中：

dyz_1——第一权限范围值；

bm——访问人员的部门赋值；

zw——访问人员的职位赋值；

zj——访问人员的职级赋值；

a_1、a_2、a_3——根据实际需求设定的权重系数。

b) 获取访问人员的职责状态信息中的参与项目类型，参与项目类型包括大型项目、中型项目和小型项目，同时获取参与项目类型的次数和负责程度，并将其分别标定为参频值 cs_c 和参深值fz_c，c 表示参与项目类型的编号，且 $c = 1,2,3$，当 $c = 1$ 时，则表示为大型项目，当 $c = 2$ 时，则表示为中型项目，当 $c = 3$ 时，则表示为小型项目，取其数值，得到第二权范值 dyz_2，计算公式如下：

$$dyz_2 = \left(\frac{cs_1}{\sum_{c=1}^{3} cs_c} \times b_1 + fz_1 \times b_2\right) \times \mu_1 + \left(\frac{cs_2}{\sum_{c=1}^{3} cs_c} \times b_3 + fz_2 \times b_4\right) \times \mu_2 + \left(\frac{cs_1}{\sum_{c=1}^{3} cs_c} \times b_5 + fz_3 \times b_6\right) \times \mu_3 \quad \text{.....(2)}$$

式（2）中：

dyz_2——第二权限范围值；

cs_c——参与项目类型的次数，即参频值；

fz_c——参与项目类型的负责程度，即参深值；

c——参与项目类型的编号；

b_1、b_2、b_3、b_4、b_5、b_6——根据实际需求设定的权重系数；

μ_1、μ_2、μ_3——分别表示设定的修正系数。

c) 提取第一权范值dyz_1和第二权范值dyz_2的数值进行归一化处理得到访问人员的访匹值 FPZ，计算公式如下：

$$FPZ = \left(\frac{1}{e}\right)^{dyz_1 \times \eta_1 + dyz_2 \times \eta_2} \quad \text{.....(3)}$$

式（3）中：

FPZ——访问人员的访匹值；

e——自然常数；

η_1、η_2——分别表示第一权范值和第二权范值的权重系数；

1） 若 $FPZ < F_1$ ，则访问人员匹配的权限范围为三级权限范围；

2） 若 $F_1 \leq FPZ < F_2$ ，则访问人员匹配的权限范围为二级权限范围；

3） 若 $FPZ \geq F_2$ ，则访问人员匹配的权限范围为一级权限范围。

d) 由一级权限范围、二级权限范围和三级权限范围构成访问人员所匹配的权限范围类型等级。

8.3.2.2 应根据权限范围类型等级，精准匹配对应范围的数字档案文件，确保访问人员仅能访问授权资料。

8.3.3 档案访问管理功能

8.3.3.1 应实时获取数字档案文件的被点击次数、运载速率和访问时长，计算访问状态评估值，实现异常数字档案文件的自动识别与标记。

8.3.3.2 针对异常数字档案文件应能触发访问限制指令，通过访限值与访限状态判定表对照，确定访限人数并发送至访问排序模块。

8.3.3.3 对各数字档案文件的访问状态分析过程如下：

a) 通过获取当前监测时段内各数字档案文件的被点击次数、运载速率和访问时长，并提取三者数值进行归一化处理，得到各数字档案文件的访问状态评估值；

b) 将各数字档案文件的访问状态评估值与访问状态评估阈值进行比较分析，若各数字档案文件的访问状态评估值大于或等于访问状态评估阈值 FY 时，则生成访问异常信号；

c) 将捕捉到访问异常信号的数字档案文件标记为异常数字档案文件，由此得到当前监测时段内各异常数字档案文件；

d) 依据当前监测时段内各异常数字档案文件生成的访问异常信号，则触发访问限制指令，依据触发的访问限制指令，则调取当前监测时段内各异常数字档案文件的访问状态评估值，并将当前监测时段内各异常数字档案文件的访问状态评估值与访问状态评估阈值进行差值计算，得到当前监测时段内各异常数字档案文件的访限值；

e) 将当前监测时段内各异常数字档案文件的访限值与存储在云数据库中的访限状态判定表进行对照匹配分析，由此得到当前监测时段内各异常数字档案文件的访限状态等级，且得到的当前监测时段内每个异常数字档案文件的访限值均对应一个访限状态等级，同时将其与访限状态等级对应的访限人数进行匹配，得到当前监测时段内各异常数字档案文件对应的访限人数。

8.3.4 访问人员管理功能

应能获取访问人员位置信息，筛选出位于允许访问异常数字档案文件地理位置范围内的可选访问人员。通过采集可选访问人员的点击时值、历访值和第二权范值，计算优选值并降序排列，按访限人数选取目标访问人员。访问人员分析过程如下：

a) 通过对访问人员的位置信息进行获取，得到访问人员的位置信息，将位于允许访问该异常数字档案文件地理位置范围内的访问人员标定为可选访问人员，获取可选访问人员的点击时值、历访值和第二权范值，并分别标记为 dsz、lfz 和 dyz_2，提取三者数值进行归一化处理，得到可选访问人员的优选值 PXA，计算公式如下：

$$PXA = log\ \frac{lfz \times \beta_2 + dyz_2 \times \beta_3}{dsz \times \beta_1} \quad \text{(4)}$$

式（4）中：

PXA——可选访问人员的优选值；

dsz——可选访问人员的点击时值；

lfz——访问人员的历访值；

β_1、β_2、β_3——分别表示点击时值、历访值和第二权范值的比例系数。

a) 通过获取当前监测时段内各异常数字档案文件可选访问人员的优选值，按照优选值的数值大小进行降序排列得到可选访问人员排列表，在可选访问人员列表中，从最高优选值开始，依次选取与各异常数字档案文件所对应访限人数相匹配的可选访问人员，将被成功选取的可选访问人员标定为当前监测时段内各异常数字档案文件的目标访问人员。

8.3.5 个性化推送管理功能

应能监测访问人员的回访次数、停留时长和深击次数，计算访行倾值，结合倾向目标词的访问时长和点击次数计算访需倾值，得到综合访倾值。并根据综合访倾值与综合访倾状态判定表对照，匹配可推送数字档案文件，实现个性化推送。数字档案文件个性化推送分析过程如下：

a) 通过获取访问人员在当前监测时段内访问各数字档案文件的回访次数、停留时长和深击次数，并将其分别标记为 hfz_p、tsz_p 和 sjz_p，p 表示各数字档案文件的编号 $p = 1,2,3.....n$，n表示各数字档案文件编号的总数，并提取三者的数值进行归一化处理得到访行倾值 W_{p1}，计算公式如下：

$$W_{p1} = 2\sqrt{e}\left(\frac{hfz_p}{hfz_p^*} \times \delta_1 + \frac{tsz_p}{tsz_p^*} \times \delta_2 + \frac{sjz_p}{sjz_p^*} \times \delta_3\right) \quad .....(5)$$

式（5）中：

W_{p1}——访行倾值；

hfz_p——回访次数；

tsz_p——停留时长；

sjz_p——深击次数；

hfz_p^*——参考回访次数；

tsz_p^*——参考停留时长；

sjz_p^*——参考深击次数；

δ_1——回访次数的权重系数；

δ_2——停留时长的权重系数；

δ_3——深击次数的权重系数。

a) 将访问人员在当前监测时段内访问各数字档案文件的访行倾值与预设的访行倾阈值进行比较分析，当访问人员在当前监测时段内访问各数字档案文件的访行倾值大于预设的访行倾阈值时，则将该数字档案文件判定为访问倾向数字档案文件，同时提取访问倾向数字档案文件的主题文本数据，文本数据为一组词语、一组评论或一段话，将文本数据中无关字符、标点符号和停用词进行去除，并将去除后的文本数据进行重新组合并分割成词语进行排序，统计分割后相关词语出现的次数，并按照词频从高到低进行排序，设置词频阈值，将词频大于词频阈值的词语标记为倾向目标词，提取访问人员在当前监测时段内访问倾向目标词的时长和点击次数的数值并将其分别乘以对应的权重系数再相加得到访需倾值记为 W_{p2}；

b) 提取访问人员的访行倾值 W_{p1} 和访需倾值记为 W_{p2} 的数值进行归一化处理，得到综合访倾值TJZ，计算公式如下：

$$TJZ = W_{p1} \times \varphi_1 + W_{p2} \times \varphi_2 \quad ..... (6)$$

式中：

TJZ——综合访倾值；

W_{p2}——访需倾值；

φ_1、φ_2——分别表示访行倾值和访需倾值的权重系数，且$\varphi_1 > \varphi_2$。

c) 将综合访倾值与预设的综合访倾阈值进行比较分析，若综合访倾值大于或等于预设的综合访倾阈值时，则进行数字档案文件个性化推送；

d) 通过将访问人员的综合访倾值与存储在云数据库中的综合访倾状态判定表进行对照分析，由此得到访问人员的综合访倾状态等级，且得到的每个访问人员的综合访倾值均对应一个综合访倾状态等级，同时将其与综合访倾状态等级对应的数字档案文件进行匹配，得到可推送数字档案文件。

8.3.6 数据存储管理功能

8.3.6.1 安全存储访问人员个人信息、权限范围类型等级、异常数字档案文件访限人数、目标访问人员、可推送数字档案文件及各类判定表等数据。

8.3.6.2 支持数据的备份、恢复及查询操作，确保数据的完整性和可用性。

8.4 性能要求

8.4.1 响应时间

数字档案资料管理系统响应时间要求如下：

a) 常规权限查询与档案访问请求响应时间 ≤ 2 s；
b) 异常数字档案文件识别与访限人数计算响应时间 ≤ 5 s；
c) 目标访问人员选择与个性化推送分析响应时间 ≤ 3 s

8.4.2 处理能力

数字档案资料管理系统处理能力要求如下：

a) 系统同时处理能力应 ≥ 1 000 个访问人员的并发访问请求；
b) 系统每日应能完成 ≥ 10 000 条数字档案资料的采集、整理与存储；
c) 系统应支持 ≥ 100 GB 数字档案资料的实时分析与处理。

8.4.3 可靠性

数字档案资料管理系统可靠性要求如下：

a) 系统连续运行时间 ≥ 99.9%，年均故障时间 ≤ 5 h；
b) 数据备份与恢复成功率 100%，确保数据在丢失或损坏时可完整恢复。

9 安全管理

9.1 访问控制

9.1.1 应建立用户身份认证机制，采用用户名/密码、数字证书、动态口令等多种认证方式，确保用户身份的真实性和合法性。

9.1.2 应根据用户的角色和职责，设置不同的访问权限，对数字档案资料的查看、下载、修改、删除等操作进行严格控制。

9.1.3 应定期对用户账号和权限进行审查和更新，及时删除或停用离职人员的账号。

9.1.4 应实时监测数字档案文件的访问状态，对异常访问（如频繁点击、异常运载速率、超长访问时长）及时触发访问限制指令。

9.2 数据加密

9.2.1 对存储在系统中的数字档案资料进行加密存储，采用先进的加密算法（如 AES 加密算法），防止数据被非法窃取和篡改。

9.2.2 在数据传输过程中，采用安全的传输协议（如 HTTPS 协议），对传输的数据进行加密，确保数据在传输过程中的安全性。

9.3 安全审计

9.3.1 应建立安全审计机制，对用户对数字档案资料的所有操作进行记录和审计，日志保存时间应 ≥ 5 年包括操作时间、操作人、操作内容、操作结果等。

9.3.2 审计日志应定期进行分析和审查，及时发现潜在的安全风险和违规操作行为，并采取相应的措施进行处理。

9.3.3 审计日志应长期保存，保存期限应符合相关法律法规和行业标准的要求。

9.4 数据备份与恢复

9.4.1 制定完善的数据备份策略，定期对数字档案资料进行全量备份和增量备份，备份数据应存储在异地安全场所，防止因本地灾难导致数据丢失。

9.4.2 建立数据恢复机制，在数据发生丢失或损坏时，能够快速、准确地从备份数据中恢复数据，确保系统的正常运行和数字档案资料的可用性。定期进行数据恢复演练，验证备份数据的有效性和恢复流程的可行性。

10 系统运维管理

10.1 系统监控

10.1.1 对数字档案资料管理系统的运行状态进行实时监控，包括服务器性能（如 CPU 使用率、内存使用率、磁盘 I/O 等）、网络状态（如网络流量、网络延迟等）、系统服务状态（如数据库服务、应用服务等）。

10.1.2 设置监控阈值，当系统运行指标超出阈值时，及时发出警报通知系统管理员，以便采取相应的措施进行处理，保障系统的稳定运行。

10.2 故障管理

10.2.1 建立故障报告和处理机制，当系统发生故障时，用户或系统监控人员能够及时报告故障情况，系统管理员应迅速响应，对故障进行诊断和排除。

10.2.2 对故障处理过程进行记录，包括故障发生时间、故障现象、故障原因、处理措施、处理时间等，以便对故障进行分析和总结，提高系统的可靠性和稳定性。

10.3 系统升级与优化

10.3.1 根据业务需求和技术发展，定期对数字档案资料管理系统进行升级和优化，包括功能升级、性能优化、安全漏洞修复等。

10.3.2 在系统升级前，应进行充分的测试和评估，制定详细的升级计划和回退方案，确保系统升级过程的顺利进行，避免对业务造成影响。

10.3.3 对系统升级和优化后的效果进行跟踪和评估，根据实际情况进一步调整和完善系统。