

数 字 山 东 工 程 标 准

SZSD 0019—2024

政务信息系统灾备指南

Guidelines for disaster recovery of government information systems

2024 - 04 - 15 发布

2024 - 06 - 01 实施

目 次

前言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 分类分级..... 1

 4.1 系统重要性分类..... 1

 4.2 灾难恢复能力分级..... 1

5 灾备策略..... 2

 5.1 概述..... 2

 5.2 本地高可用..... 2

 5.3 本地备份..... 2

 5.4 异地备份..... 2

 5.5 同城灾备..... 3

6 策略实施..... 3

7 灾备演练..... 3

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。

本文件由山东省大数据局提出、归口并组织实施。

本文件起草单位：北京邮电大学、山东省齐鲁大数据研究院、山东新一代标准化研究院有限公司、山东省大数据局、山东省大数据中心、华为技术有限公司、浪潮云信息技术股份公司、上海爱数信息技术股份有限公司、上海英方软件股份有限公司。

本文件主要起草人：辛阳、朱效民、魏淑斌、张荣光、赵硕、张继辉、陈克磊、谢枫、张浩秋。

政务信息系统灾备指南

1 范围

本文件给出了政务信息系统分类分级、灾备策略、策略实施、灾备演练等方面指导建议。
本文件适用于为政务信息系统灾备工作提供指导。

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 20988—2007 信息安全技术 信息系统灾备恢复规范
GB/T 31167—2014 信息安全技术 云计算服务安全指南
GB/T 36957—2018 信息安全技术灾难恢复服务要求
SZSD 0020—2024 灾备节点技术要求

3 术语和定义

SZSD 0020—2024界定的术语和定义适用于本文件。

4 分类分级

4.1 系统重要性分类

根据业务影响分析的结果，确定系统重要性，系统重要性分类参见GB/T 31167—2014的6.4节。业务影响分析主要包括：

- 业务核心功能分析：宜包括业务服务范围、数据集中程度、业务时间敏感性等方面；
- 依赖性分析：宜对政务信息系统的应用架构、关键资源模块、业务数据流及支撑基础架构进行分析。确认业务系统、应用系统环境、系统之间依赖关系、关键资源等系统信息，并对应用系统为适应灾难恢复需求而进行的改造提出建议；
- 业务中断影响分析：宜采用定量和定性分析的方法，对各种业务功能中断所可能造成的影响进行评估，依据 GB/T 20988—2007 中 5.2.2 节。

4.2 灾难恢复能力分级

4.2.1 风险分析的目标为政务信息系统所处的运行环境，评估内容包括数据中心场地、系统、应用、主机、网络、存储等运行支撑环境及相关技术支持与运维管理能力的实际状况。

4.2.2 根据风险分析结果确定不同系统的灾难恢复能力等级，灾难恢复能力等级见 GB/T 20988—2007 的附录 A。

4.2.3 不同政务信息系统对应不同的灾难恢复能力分级，对应关系见表 1。

表 1 对应关系

系统重要性分类	灾难恢复能力分级
一般信息系统	第1级 基本支持
重要信息系统	第2级 备用场地支持
	第3级 电子传输和部分设备支持
	第4级 电子传输及完整设备支持
关键信息系统	第5级 实时数据传输及完整设备支持
	第6级 数据零丢失和远程集群支持

5 灾备策略

5.1 概述

根据政务信息系统分类分级，确定相应的灾备策略，灾备策略包括本地高可用、本地备份、异地备份、同城灾备等方法，灾备策略见表2。

表 2 灾难策略

系统重要性分类	灾难恢复能力分级	本地高可用	本地备份	异地备份	同城灾备
一般信息系统	第1级 基本支持	无需	重要数据必需	无需	无需
重要信息系统	第2级 备用场地支持	无需	重要数据必需	无需	无需
	第3级 电子传输和部分设备支持	无需	重要数据必需	无需	无需
	第4级 电子传输及完整设备支持	必需	重要数据必需	重要数据必需	无需
关键信息系统	第5级 实时数据传输及完整设备支持	必需	重要数据必需	重要数据必需	无需
	第6级 数据零丢失和远程集群支持	必需	重要数据必需	重要数据必需	必需

5.2 本地高可用

在本地数据中心建立冗余政务信息系统，日常情况下可同时分担业务及管理系统的运行，减少系统中断时间，保障服务高度可用性。

5.3 本地备份

将重要数据通过在线备份的方式储存到本地另一个位置，并确保政务信息系统产生的数据与本地备份数据隔离。

5.4 异地备份

将本地备份数据通过电子政务外网复制至异地灾备节点，当本地数据中心故障导致数据损毁时，可基于异地备份数据进行数据恢复，异地备份策略宜符合表3的相关规定。

表 3 异地备份策略

配置项	备份策略
备份方式	对象存储选择“全量”备份；数据库建议选择“全量+增量”备份
备份时间	可设置为任意时间段，以小时为单位，建议在业务低峰期进行数据备份
备份恢复方式	按备份集恢复数据

5.5 同城灾备

5.5.1 数据备份策略

数据备份策略包括但不限于：

- a) 按需申请同城灾备资源，将本地备份数据通过电子政务外网复制至同城灾备节点；
- b) 提供实例地址，保障跨数据中心高可用性。

5.5.2 应用容灾策略

应用容灾策略包括但不限于：

- a) 按需在同城灾备节点部署业务应用，并通过跨数据中心负载均衡对外提供服务；
- b) 通过域名访问不同数据中心里的各类政务云服务，如政务云服务切换到备数据中心时，云服务的域名不变，应用无需改造；
- c) 系统宜配置网络重试机制，以降低会话中断风险；
- d) 系统正式上线前宜对系统试运行，测试和验证应用容灾服务能力。

6 策略实施

灾难策略实施宜参考GB/T 36957—2018中第6.2和6.3节的相关内容，满足灾难恢复服务过程要求。

7 灾备演练

7.1 制定演练预案，预案内容包括确定灾难恢复的范围和目标、灾难恢复的总体规程、灾难恢复步骤和业务功能恢复验证测试方法等。

7.2 演练内容包括数据验证和应用验证，具体包括：

- a) 数据验证内容包括数据的可用性和一致性；
- b) 应用验证内容包括启动灾备系统的磁盘卷组、数据库及中间件等，确认其运行状态。

7.3 演练方式分为桌面演练、模拟演练和实战演练，演练要求见GB/T 36957的相关要求；

7.4 在演练过程中及时记录形成文档报告。
