|  |  |
| --- | --- |
| ICS  | L80 |
| CCS  |

|  |
| --- |
| D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png GXIE |

35.220.01 |

广西电子学会团体标准

T/XXX XXXX—XXXX

网络安全技术 气象行业灾备能力建设规范

Network Security Technology Specification for the Construction of Disaster Recovery System for Information Systems in the Meteorological Industry

XXXX - XX - XX发布

XXXX - XX - XX实施

广西电子学会  发布

目次

[前言 IV](#_Toc194072470)

[1 范围 1](#_Toc194072471)

[2 规范性引用文件 1](#_Toc194072472)

[3 术语和定义 1](#_Toc194072473)

[4 灾备能力体系建设要求 1](#_Toc194072474)

[4.1 总体目标与原则 1](#_Toc194072475)

[4.1.1 总体目标 1](#_Toc194072476)

[4.1.2 建设原则 1](#_Toc194072477)

[4.2 业务连续性要求 2](#_Toc194072478)

[4.2.1 关键业务识别 2](#_Toc194072479)

[4.2.2 恢复优先级设定 2](#_Toc194072480)

[4.3 技术可靠性要求 2](#_Toc194072481)

[4.3.1 硬件设备稳定性 2](#_Toc194072482)

[4.3.2 软件系统兼容性 2](#_Toc194072483)

[4.4 网络信息安全性要求 2](#_Toc194072484)

[4.4.1 网络安全防护 2](#_Toc194072485)

[4.4.2 数据安全保障 3](#_Toc194072486)

[4.4.3 安全管理体系 3](#_Toc194072487)

[5 灾备能力体系规划与设计 3](#_Toc194072488)

[5.1 风险分析与评估 3](#_Toc194072489)

[5.1.1 灾难风险识别 3](#_Toc194072490)

[5.1.2 风险影响评估 3](#_Toc194072491)

[5.1.3 风险优先级排序 3](#_Toc194072492)

[5.2 信息系统灾难恢复目标 3](#_Toc194072493)

[5.2.1 恢复时间目标（RTO） 3](#_Toc194072494)

[5.2.2 恢复点目标（RPO） 4](#_Toc194072495)

[5.3 灾备业务连续性方案 4](#_Toc194072496)

[5.3.1 业务切换机制 4](#_Toc194072497)

[5.3.2 业务恢复验证 4](#_Toc194072498)

[5.4 灾备系统布局方案 4](#_Toc194072499)

[5.4.1 本地灾备 4](#_Toc194072500)

[5.4.2 同城灾备 4](#_Toc194072501)

[5.4.3 异地灾备 4](#_Toc194072502)

[5.4.4 云灾备 4](#_Toc194072503)

[5.4.5 混合灾备 5](#_Toc194072504)

[5.5 灾备基础设施方案 5](#_Toc194072505)

[5.5.1 机房环境方案 5](#_Toc194072506)

[5.5.2 数据存储方案 5](#_Toc194072507)

[5.5.3 网络与通信方案 5](#_Toc194072508)

[5.5.4 电力供应方案 5](#_Toc194072509)

[5.5.5 安全防护方案 5](#_Toc194072510)

[5.6 灾备应急联动方案 5](#_Toc194072511)

[5.6.1 跨部门联动灾备机制 5](#_Toc194072512)

[5.6.2 数据共享灾备机制 5](#_Toc194072513)

[5.6.3 数据安全与权限管理方案 5](#_Toc194072514)

[6 灾备能力体系实施与演练 5](#_Toc194072515)

[6.1 预案制定 5](#_Toc194072516)

[6.1.1 灾备预案分类与内容 6](#_Toc194072517)

[6.1.2 预案制定流程与要求 6](#_Toc194072518)

[6.1.3 预案文档化管理 6](#_Toc194072519)

[6.2 预案审核 6](#_Toc194072520)

[6.2.1 预案审核流程 6](#_Toc194072521)

[6.2.2 预案审核标准 6](#_Toc194072522)

[6.2.3 预案审核结果处理 6](#_Toc194072523)

[6.3 预案发布 6](#_Toc194072524)

[6.3.1 预案发布流程 6](#_Toc194072525)

[6.3.2 预案版本管理 7](#_Toc194072526)

[6.3.3 预案宣传与培训 7](#_Toc194072527)

[6.4 测试计划与执行 7](#_Toc194072528)

[6.4.1 测试计划制定 7](#_Toc194072529)

[6.4.2 测试执行与记录 7](#_Toc194072530)

[6.4.3 测试结果分析与改进 7](#_Toc194072531)

[6.5 演练计划与执行 7](#_Toc194072532)

[6.5.1 演练计划制定 7](#_Toc194072533)

[6.5.2 演练实施与记录 7](#_Toc194072534)

[6.5.3 演练评估与总结 7](#_Toc194072535)

[7 灾备能力体系评估与改进 7](#_Toc194072536)

[7.1 灾备评估指标 7](#_Toc194072537)

[7.1.1 技术指标 7](#_Toc194072538)

[7.1.2 管理指标 8](#_Toc194072539)

[7.2 灾备能力评估 8](#_Toc194072540)

[7.2.1 评估机制 8](#_Toc194072541)

[7.2.3 灾备审计 8](#_Toc194072542)

[7.3 灾备改进与更新 8](#_Toc194072543)

[7.3.1 问题识别与分析 8](#_Toc194072544)

[7.3.2 改进计划制定与实施 8](#_Toc194072545)

[7.3.3 改进效果跟踪与验证 9](#_Toc194072546)

[8 灾备能力体系人员培训 9](#_Toc194072547)

[8.1 灾备知识教育 9](#_Toc194072548)

[8.1.1 灾备基础知识普及 9](#_Toc194072549)

[8.1.2 灾备意识提升 9](#_Toc194072550)

[8.1.3 灾备文化建设 9](#_Toc194072551)

[8.2 灾备人才培训 9](#_Toc194072552)

[8.2.1 专业技能培训 9](#_Toc194072553)

[8.2.2 管理能力培训 9](#_Toc194072554)

[8.2.3 应急响应与处置培训 9](#_Toc194072555)

[附录A（规范性） 灾难恢复能力等级划分 11](#_Toc194072556)

[附录B（资料性） 灾难恢复预案框架 12](#_Toc194072557)

[B.1 目标和范围 12](#_Toc194072558)

[B.2 组织和职责 12](#_Toc194072559)

[B.3 联络与通讯 12](#_Toc194072560)

[B.4 突发事件响应流程 12](#_Toc194072561)

[B.4.1 事件通告 12](#_Toc194072562)

[B.4.2 人员疏散 12](#_Toc194072563)

[B.4.3 损害评估 12](#_Toc194072564)

[B.4.4 灾难宣告 12](#_Toc194072565)

[B.5 恢复及重续运行流程 12](#_Toc194072566)

[B.5.1 恢复 12](#_Toc194072567)

[B.6 后重建和回退 12](#_Toc194072568)

[B.7 预案的保障条件 12](#_Toc194072569)

[B.8 预案附录 13](#_Toc194072570)

[附录C（资料性） 灾难恢复预案框架 14](#_Toc194072571)

[附录D（资料性） 某行业RTO/RPO与灾难恢复能力等级的关系示例 15](#_Toc194072572)

[D.1 RTO/RPO与灾难恢复能力等级的关系 15](#_Toc194072573)

1. 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。

本文件由广西电子学会提出、归口并宣贯。

本文件起草单位：广西壮族自治区气象信息中心、广西通信规划设计咨询有限公司、广西讯纳电子科技有限公司、飞创信息科技有限公司。

本文件主要起草人：林健玲、李育晖、邓景倍、农欣、许卉、庞力荣、苏芳来、马军、刘桨、邓力涌、王倩、肖红飞、周恩沿。

网络安全技术 气象行业灾备能力建设规范

* 1. 范围

本文件规定气象行业领域的灾备能力建设应遵循的基本要求。

本文件适用于气象行业灾备能力建设的规划与设计、实施和管理。

* 1. 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 20269 信息安全技术 信息系统安全管理要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22239 网络安全等级保护基本要求

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 30285 信息安全技术 灾难恢复中心建设与运维管理规范

GB/T 32914 信息安全技术 网络安全服务能力要求

GB/T 36957 信息安全技术 灾难恢复服务要求

GB/T 37046 信息安全技术 灾难恢复服务能力评估准则

DB41/T 2680.3 气象灾害防御 第3部分：重点单位气象安全能力建设要求

T/GXIE 006 网络安全技术 信息系统灾备体系 术语

T/XBLM 0001 数据备份与恢复能力成熟度

关键农时气象服务通则

气象观测质量管理体系

气象网络安全管理制度

气象站恢复与业务技能提升专项协议

* 1. 术语和定义

T/GXIE 006界定的术语和定义适用于本文件。

* 1. 灾备能力体系建设要求
		1. 总体目标与原则
			1. 总体目标
			2. 建设原则
		2. 业务连续性要求
			1. 关键业务识别
			2. 恢复优先级设定
		3. 技术可靠性要求
			1. 硬件设备稳定性
			2. 软件系统兼容性
		4. 网络信息安全性要求
			1. 网络安全防护
			2. 数据安全保障
			3. 安全管理体系
	2. 灾备能力体系规划与设计
		1. 风险分析与评估
			1. 灾难风险识别
			2. 风险影响评估
			3. 风险优先级排序
		2. 信息系统灾难恢复目标
			1. 恢复时间目标（RTO）

结合气象行业关键业务的风险场景等级及优先级排序，对不同风险场景分别设定不同的RTO。

1. 不同场景的恢复时间目标（RTO）

| 序号 | 风险等级 | 风险场景 | RTO |
| --- | --- | --- | --- |
| 1 | 高风险 | 如气象灾害预警系统中断、气象数据中心故障、恶意攻击导致数据篡改等直接影响国家安全或社会运行的核心业务 | RTO≤15 分钟 |
| 2 | 中风险 | 如区域气象服务瘫痪、影响地方应急响应、交通调度及农业生产等支撑行业运转的重要业务 | RTO≤1 小时 |
| 3 | 低风险 | 如办公系统故障、非实时气象数据备份丢失、气象设备维护延迟等辅助性或区域性服务的一般业务 | RTO≤24 小时 |

* + - 1. 恢复点目标（RPO）

结合气象行业风险等级、业务重要性、恢复成本等因素，对不同风险场景分别设定不同的RPO。

1. 不同场景的恢复点目标（RPO）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 风险等级 | 风险场景 | RTO |
| 1 | 高风险 | 如气象灾害预警系统中断、气象数据中心故障、恶意攻击导致数据篡改等直接影响国家安全或社会运行的核心业务 | 小于1小时 |
| 2 | 中风险 | 如区域气象服务瘫痪、影响地方应急响应、交通调度及农业生产等支撑行业运转的重要业务 | 1小时至4 小时 |
| 3 | 低风险 | 如办公系统故障、非实时气象数据备份丢失、气象设备维护延迟等辅助性或区域性服务的一般业务 | 4小时至24 小时 |

* + 1. 灾备业务连续性方案
			1. 业务切换机制
			2. 业务恢复验证
		2. 灾备系统布局方案
			1. 本地灾备

部署本地备份存储设备（如分布式存储集群），应对单点设备故障或短时数据中断，保障实时气象要素（如雷达、卫星数据）的本地快速恢复。

* + - 1. 同城灾备
			2. 异地灾备
			3. 云灾备
			4. 混合灾备
		1. 灾备基础设施方案
			1. 机房环境方案
			2. 数据存储方案
			3. 网络与通信方案
			4. 电力供应方案
			5. 安全防护方案
		2. 灾备应急联动方案
			1. 跨部门联动灾备机制
			2. 数据共享灾备机制
			3. 数据安全与权限管理方案
	1. 灾备能力体系实施与演练
		1. 预案制定
			1. 灾备预案分类与内容
1. 标题

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 预案类别 | 适用场景 | 主要内容 |
| 1 | 事件响应类 | 突发灾害（如台风、地震） | 应急指挥体系、灾情评估流程、优先级业务恢复顺序、人员疏散与安全保障措施。 |
| 2 | 业务恢复类 | 系统故障或数据中断 | 数据回滚策略、主备切换操作步骤、恢复验证标准（如数据一致性阈值≤0.1%差异）。 |
| 3 | 资源调度类 | 基础设施损毁（供电、网络） | 备用设备调用清单、供应商联络机制、临时通信链路搭建方案（如卫星终端启用）。 |
| 4 | 协同处置类 | 跨区域或多部门联动场景 | 外部机构协作接口人清单、信息共享协议、联合指挥调度流程。 |

* + - 1. 预案制定流程与要求
			2. 预案文档化管理
		1. 预案审核
			1. 预案审核流程
			2. 预案审核标准
			3. 预案审核结果处理
		2. 预案发布
			1. 预案发布流程
			2. 预案版本管理

应采用“年份-版本号-修订日期”命名规则，历史版本保留≥5年，修订记录应标注变更内容、责任人及依据。主版本存于独立文档库（支持全文检索），旧版本标记为“失效”但禁止删除。

* + - 1. 预案宣传与培训
		1. 测试计划与执行
			1. 测试计划制定
			2. 测试执行与记录
			3. 测试结果分析与改进
		2. 演练计划与执行
			1. 演练计划制定
			2. 演练实施与记录
			3. 演练评估与总结
	1. 灾备能力体系评估与改进
		1. 灾备评估指标
			1. 技术指标
			2. 管理指标
			3. 评估机制

评估方法

* + - 1. 灾备审计
		1. 灾备改进与更新
			1. 问题识别与分析
			2. 改进计划制定与实施
			3. 改进效果跟踪与验证
	1. 灾备能力体系人员培训
		1. 灾备知识教育
			1. 灾备基础知识普及
			2. 灾备意识提升
			3. 灾备文化建设
		2. 灾备人才培训
			1. 专业技能培训
			2. 管理能力培训
			3. 应急响应与处置培训
1.
2. （规范性）
灾难恢复能力等级划分

基本支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第1级要求，要求至少每周进行一次数据备份，并确保备份介质场外存放。这是灾难恢复的最基础级别，主要关注数据的定期备份。

备用场地支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第2级要求，在满足基本支持的条件基础上要求配备灾难恢复所需的部分数据处理设备，或灾难发生后能在预定时间内调配所需的数据处理设备到备用场地。

电子传输和设备支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第3级要求，要求每天至少进行一次完全数据备份，并利用通信网络将关键数据定时批量传送至备用场地。同时，需要配备灾难恢复所需的部分数据处理设备、通信线路和相应的网络设备。

电子传输及完整设备支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第4级要求，在上一级的基础上要求配置灾难恢复所需的所有数据处理设备、通信线路和相应的网络设备，并且处于就绪或运行状态。

实时数据传输及完整设备支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第5级要求，在上一级的基础上除了要求每天至少进行一次完全数据备份外，还要求采用远程数据复制技术，利用通信网络将关键数据实时复制到备用场地。

数据零丢失和远程集群支持：需满足国标《信息系统灾难恢复规范》(GB/T 20988-2007)灾难恢复等级第6级要求，在上一级的基础上要求实现远程实时备份，数据零丢失；备用数据处理系统具备与生产数据处理系统一致的处理能力，应用软件是“集群的”，可实时无缝切换。

1. （资料性）
灾难恢复预案框架
	1. 目标和范围

定义灾难恢复预案中的相关术语和方法论，并说明灾难恢复的目标，如恢复时间目标（RTO）和恢复点目标（RPO）。说明预案的作用范围，解决哪些问题，不解决哪些问题。

* 1. 组织和职责

描述灾难恢复组织的组成、各个岗位的职责和人员名单。灾难恢复组织应包括应急响应组、灾难恢复组等。

* 1. 联络与通讯

列出灾难恢复相关人员和组织的联络表。包含灾难恢复团队、运营商、厂商、主管部门、媒体、员工家属等。联络方式包括固定电话、移动电话、对讲机、电子邮件和住址等。

* 1. 突发事件响应流程
		1. 事件通告

任何人员在发现信息系统相关突发事件发生或即将发生时，应按预定的流程报告相关人员，并由相关人员进行初步判断、通知和处置。

* + 1. 人员疏散

提供指定的集合地点和替代的集合地点，还包括通知人员撤离的办法，撤离的组织和步骤等。

* + 1. 损害评估

在突发事件发生后，应由应急响应组的损害评估人员，确定事态的严重程度。由灾难恢复责任人召集相应的专业人员对突发事件进行慎重评估，确认突发事件对信息系统造成的影响程度，确定下一步将要采取的行动。一旦系统的影响被确定，应将最新信息按照预定的通告流程通知给相应的团队。

* + 1. 灾难宣告

应预先制定灾难恢复预案启动的条件。当损害评估的结果达到一项或多项启动条件时，组织将正式发出灾难宣告，宣布启动灾难恢复预案，并根据宣告流程通知各有关部门。

* 1. 恢复及重续运行流程
		1. 恢复

按照业务影响分析中确定的优先顺序，在灾难备份中心恢复支持关键业务功能的数据、数据处理系统和网络系统。描述时间、地点、人员、设备和每一步的详细操作步骤，同时还包括特定情况发生时各团队之间进行协调的指令，以及异常处理流程。

灾难备份中心的系统替代主系统，支持关键业务功能的提供。这一阶段包含主系统运行管理所涉及的主要工作，包含重续运行的所有操作流程和规章制度。

* 1. 后重建和回退

最后阶段是主中心的重建工作，中止灾难备份系统的运行，回退到组织的主系统。

* 1. 预案的保障条件

预案的保障条件如下：

1. 专业技术保障；
2. 通信保障；
3. 后勤保障。
	1. 预案附录

预案的附录如下：

1. 人员疏散计划；
2. 产品说明书；
3. 信息系统标准操作流程；
4. 服务级别协议和备忘录；
5. 资源清单；
6. 业务影响分析报告；
7. 预案的保存和分发办法。
8. （资料性）
某行业RTO/RPO与灾难恢复能力等级的关系示例
	1. RTO/RPO与灾难恢复能力等级的关系

参考《信息系统灾难恢复规范》(GB/T 20988-2007)，表C.1说明信息系统灾难恢复各等级对应的RTO/RPO范围。

* 1. RTO/RPO 与灾难恢复能力等级的关系

|  |  |  |
| --- | --- | --- |
| **灾难恢复能力等级** | **RTO** | **RPO** |
| 1 | 2天以上 | 1天至7天 |
| 2 | 24小时以上 | 1天至7天 |
| 3 | 12小时以上 | 数小时至1天 |
| 4 | 数小时至2天 | 数小时至1天 |
| 5 | 数分钟至2天 | 0至30分钟 |
| 6 | 数分钟 | 0 |

