ICS 35.040
CCS L 80
备案号 87066-2022

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 08—2022

人力资源社会保障灾备中心建设和运维管理规范

Specification for disaster recovery center construction and operation and maintenance management in human resources and social security

2022-09-30 发布　　2022-12-01 实施

中华人民共和国人力资源和社会保障部　　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。

本文件由人力资源和社会保障部信息中心提出并归口。

本文件起草单位：人力资源和社会保障部信息中心。

本文件主要起草人：石永辉、成勇、张博、王祥宇、李笑男、马丹蕾、耿建军。

引　言

根据《信息系统灾难恢复规范》（GB/T 20988-2007），人力资源社会保障部在2011年制定了《人力资源和社会保障信息系统灾难恢复指南》（人社信息函[2011]4号）。为规范和引导人力资源社会保障行业灾备中心建设和运维管理工作，提高人力资源社会保障信息系统应对突发事件和灾难的能力，有效防范信息系统的风险，根据《信息系统灾难恢复规范》（GB/T 20988-2007）和《灾难恢复中心建设与运维管理规范》（GB/T 30285-2013），参考《人力资源和社会保障信息系统灾难恢复指南》，结合人力资源社会保障行业灾备建设实际情况，制定本规范。

人力资源社会保障灾备中心建设和运维管理规范

1 范围

本文件规定了人力资源社会保障灾备中心建设和运维的管理过程。

本文件适用于部本级和省级人力资源社会保障部门开展灾备中心建设和运维管理工作。

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 信息系统灾难恢复规范

GB/T 30285-2013 信息安全技术 灾难恢复中心建设与运维管理规范

人社信息函[2011]4号 人力资源和社会保障信息系统灾难恢复指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 生产系统 production system

正常情况下满足业务运营的信息系统。

3.2 灾难备份系统 disaster recovery system

用于灾难恢复目的，当灾难发生导致生产系统不可用时用于接替生产运行的信息系统，以满足业务运营的连续性要求。

3.3 数据中心 data center

用于支撑信息系统运行的场地和环境，一般由电力保障系统、空气调节系统、安全保障系统、监控系统、消防系统、机柜及桥架、办公及生活保障设施等构成。

3.4 生产中心 production center

利用数据中心场地和环境支撑生产系统运行，对重要信息进行集中管理和处理的场所和组织。

3.5 灾备中心 disaster recovery center

满足关键业务运营连续性的要求，利用数据中心场地和环境支撑灾难备份系统运行，抵御导致生产系统全部或部分不可用的灾难，用以接替生产中心部分或全部职能，对重要信息进行集中管理和处理的场所和组织。

注：灾备中心按照其风险防范职能及与生产中心的距离，可分为同城灾备中心和异地灾备中心。

3.6 同城灾备中心 city disaster recovery center

与生产中心一般处于同一城市，但与生产中心处于不同的风险区域内，能够抵御同一城市内小范围灾难的灾备中心。

注：同城灾备中心可实现同步“零数据丢失”复制，抵御较小范围风险。

3.7 异地灾备中心 remote disaster recovery center

与生产中心一般处于不同城市，能够抵御较大规模的区域性灾难的灾备中心。

注：异地灾备中心可实现异步复制或定时备份方式，抵御较大范围的风险。

3.8 灾难恢复演练 disaster recovery exercises

为验证灾难备份系统的有效性，确保灾难备份系统能够顺利接替生产系统运行，需要通过演练的方式验证灾难备份系统与生产系统数据的一致性和完整性，验证灾难备份系统接替生产系统的能力。

3.9 灾难备份系统切换 disaster recovery system failover

将生产系统切换到灾难备份系统运行，利用灾备中心接管部分或全部生产中心职能的活动。

4 灾备中心组织机构

4.1 机构建立

灾备中心的组织机构应与生产中心的组织机构统筹规划,结合本单位实际,建立灾备中心组织机构，并明确岗位和职责。

4.2 机构人员

灾备中心的组织机构人员包括管理、业务、技术和行政后勤等方面人员。

4.3 机构职责

灾备中心的组织机构应负责灾备中心的建设管理和运维管理工作。其中，建设管理包括灾备中心的规划、建设和交付的管理等工作；运维管理包括灾备中心的日常运行维护、应急和切换、灾备演练的管理等工作。灾备中心的组织机构的部分职责可以通过购买服务的方式由其他社会化的服务机构支撑。

5 灾备中心需求分析和规划

5.1 灾备中心需求分析

5.1.1 生产中心风险分析

生产中心面临的风险主要包括：

a） 自然灾害；

b） 基础设施风险，包括火灾、停电、UPS 故障、空调故障等；

c） 信息系统风险，包括软件故障、硬件故障、数据丢失、人为误操作、病毒攻击等。

应分析人力资源社会保障信息系统面临的潜在风险，确定灾难备份系统建设的必要性。

5.1.2 业务影响分析

应按照 GB/T 20988-2007 和人社信息函[2011]4 号的要求,根据人力资源社会保障信息系统的情况，进行业务功能分析和业务中断影响分析。

a）业务功能分析包括：业务功能的政策性要求；业务系统服务范围；业务数据集中程度；业务系统的时间敏感性；业务功能可替代性等。

b）业务中断影响分析包括：业务中断给人力资源社会保障部门带来的各类损失，包括经济损失和社会影响（如影响政府职能、公民及法人的合法权利、公民及法人的合法经济利益、政府声誉、社会稳定）等。

通过业务影响分析，确立人力资源社会保障业务系统的灾难恢复指标(RTO 和 RPO)。通过对业务系统和信息系统的关联分析，进而确定人力资源社会保障信息系统的灾难恢复指标、灾难恢复的优先级别和灾难恢复资源需求。

5.1.3 应用关联分析

应通过对业务应用逻辑架构和业务功能的分析，明确各应用系统的关联关系，包括数据流向、信息交互方式、交互时段和交互路径等，通过应用系统关联分析，确立灾难备份的范围和灾备中心信息系统的部署方式。

5.2 灾备中心规划

5.2.1 灾难恢复策略制定

灾难备份策略制定包括：

a） 业务恢复策略制定

业务恢复策略的制定应包括业务恢复的手段和恢复流程，数据追补手段和流程，确保发生灾难时业务的持续运行。

b） 灾难恢复范围的确定

应根据人力资源社会保障业务特点，按照国家和行业相关规范的要求，依据应用系统关联分析，确定信息系统灾难恢复的范围。

c） 灾难恢复技术策略制定

应根据应用系统灾难恢复指标的要求，制定信息系统灾难恢复等级，按照 GB/T 20988—2007 信息系统灾难恢复规范中针对不同灾难恢复等级所确定的灾难恢复资源需求，制定灾难恢复的技术策略。

d） 灾难备份系统实施策略制定

按照灾难备份系统技术策略的要求，结合灾难恢复的范围，制定灾难备份系统的实施策略，包括实施原则、实施范围、实施方法、实施流程等。

e） 灾难恢复预案开发策略制定

按照灾难恢复的实施策略，结合人力资源社会保障业务特点，制定灾难恢复预案开发策略。

f） 灾备中心运维管理策略制定

针对灾难备份系统运维的要求，确定灾难备份系统运维模式、运维制度、运维团队和运维流程。

5.2.2 场地选址规划

应按照 GB/T 30285-2013 的场地选址和人社信息函[2011]4 号的灾备中心布局的要求，进行灾备中心场地选址规划。选址应服从国家战略安全要求，应避免灾备中心与生产中心处于同类风险区域。

5.2.3 资源获取规划

灾备中心基础设施资源，可采取以下方式获得：

a） 自建

人力资源社会保障部门自建基础设施并运行。

b） 购买

购买现有第三方基础设施。

c） 租用

租用第三方基础设施，并由具有信息系统灾难恢复能力的第三方机构提供运维。

灾备中心基础设施可以是物理资源或云资源，根据技术发展，可逐步采用云资源。

5.2.4 信息系统规划

应根据灾难恢复需求评估结论，结合生产中心信息系统的具体情况进行灾备中心的信息系统规划，包括灾难备份技术策略的制定、信息系统资源规划和信息系统资源部署规划。

a）灾难备份技术策略的制定：应根据灾难恢复需求评估的结论，结合生产中心信息系统的配置情况，通过对业界主流灾难备份技术的分析，按照 GB/T 20988—2007 中关于不同灾难恢复等级的各要素要求，制定适合灾难恢复需求的技术策略，包括数据备份策略、数据复制策略、系统切换策略和网络切换策略。

b）信息系统资源规划：应根据灾难备份技术策略的要求，进行灾备中心信息系统资源规划，包括备用数据处理资源规划、数据存储与备份资源规划和备用网络资源规划。

c）信息系统资源部署规划：应按照信息系统资源规划中不同信息系统资源的类型和配置的要求，进行信息系统资源部署规划，包括数据备份与复制平台的部署规划、备用数据处理资源部署规划、备用数据存储资源部署规划、备用网络资源部署规划和灾备中心应用系统部署规划。

灾难备份系统需考虑信息安全等级保护要求。按照信息安全等级保护管理规范和技术标准，灾难备份系统等级保护要求一般与生产系统保持一致。

5.2.5 方案设计

根据灾难恢复策略，进行灾备中心方案设计。包括灾难恢复技术方案和灾备中心实施方案。

a）灾难恢复技术方案设计：应根据灾备中心信息系统规划，进行灾备中心技术方案设计，包括备用数据处理系统、备用数据存储系统、备用网络方案的设计，灾备中心系统资源配置建议；灾难恢复技术方案设计应按照灾难恢复的技术策略，制定灾难备份系统的技术架构，包括数据备份与恢复技术架构、数据复制技术架构、网络技术架构、系统切换与回切技术架构等。

b）灾备中心实施方案设计：应按照灾难恢复技术方案的要求，制定灾备中心实施方案，包括实施计划、实施流程、实施管理方案和实施的风险控制等。

6 灾备中心建设管理

6.1 灾难备份系统建设管理

灾难备份系统一般包括数据存储备份系统、备份应用系统、备用网络系统。

a）数据存储备份系统

数据存储备份系统应本着数据的一致性原则进行建设，确保灾备中心与生产中心数据的一致性和完整性，在系统实施过程中，应进行必要的数据一致性和完整性验证，并考虑灾备中心备份数据的安全性。

b）备份应用系统

为满足业务持续性运行的要求，备份应用系统应在系统运行环境和软件版本等方面与生产系统完全兼容，在备份应用系统建设时，应进行系统运行能力的测试验证和切换与恢复验证，以确保灾难备份系统平台的有效性和可操作性，以及灾难备份系统接管生产系统运行的能力。

c）备用网络系统

备用网络系统的建设与实施应按照灾难备份系统规划方案的要求，对灾备中心内部网络、生产中心与灾备中心之间的互联网络、灾备中心与上级人力资源社会保障部门之间的网络、灾备中心与下级人力资源社会保障部门之间的网络平台进行实施，搭建灾难备份系统切换和恢复所需要的网络支撑环境。

6.2 预案体系建设管理

应建立有效的预案管理体系，确保预案符合应急和灾难恢复管理要求。预案体系包括应急预案体系和灾难恢复预案体系。应急预案体系用于描述在紧急情况下的应急响应和处置过程；灾难恢复预案体系用于描述在紧急情况下进行抢救和恢复的过程。

6.3 灾备中心交付管理

6.3.1 网络系统切换与回切能力验证

a） 网络设备的切换与回切能力验证

应通过技术手段进行网络设备的切换与回切的验证和测试，确保灾难发生时，灾备中心的网络能对外提供服务，以及灾后回退时生产中心的网络能提供对外服务。

b） 网络线路的切换与回切能力验证

应通过技术手段进行网络线路的切换与回切的验证和测试，确保灾难发生时，灾难恢复线路畅通，各级人力资源社会保障部门、外联单位等能够顺利连接到灾备中心，以及灾后回退时能够顺利连接到生产中心。

6.3.2 信息系统切换与回切能力验证

a） 主机操作系统切换与回切能力验证

应通过技术手段进行主机操作系统的切换与回切的验证和测试，保证灾难发生时应用系统主机能顺利切换到灾备中心，以及灾后回退时，主机也能顺利回切至生产中心。防止生产中心与灾备中心主机操作系统环境不一致，导致主机接管失败。

b） 存储系统能力验证

应通过技术手段验证灾备中心存储系统能力，保证灾难发生时，灾备中心存储系统的可访问和数据的可用性。

c） 数据库系统切换与回切能力验证

应通过技术手段进行数据库系统的切换与回切的验证和测试，保证灾难发生时，数据库系统能够顺利切换到灾备中心，以及灾后回退时，数据库系统也能回切至生产中心。

6.3.3 应用系统切换与回切能力验证

a） 灾备中心应用系统运行能力验证

应通过技术手段和业务手段对灾备中心应用系统进行验证，验证应用系统能否正常对外服务，验证应用系统数据访问能力，验证应用系统变更后的业务处理有效性。

b） 应用系统切换与回切能力验证

应通过技术手段和业务手段对灾备中心应用系统进行切换与回切的验证和演练，保证灾难发生时应用系统能够顺利切换到灾备中心，以及灾后回退时应用系统能回切至生产中心运行。

6.3.4 数据的完整性和一致性验证

应采用技术和业务手段对灾备中心数据的有效性和完整性进行验证。

应采用技术和业务手段对生产中心与灾备中心业务数据的一致性进行验证。

6.3.5 数据备份与恢复能力验证

应采用技术和业务手段对灾备中心数据备份能力进行验证，防止数据备份中断，或是数据备份周期超出设计的时间范围；同时通过技术和业务手段验证灾备中心备份数据的可恢复性，防止一旦灾难发生时备份数据失效，导致系统恢复失败。

6.3.6 灾难恢复预案的验证

灾难恢复预案至少应包含灾难恢复的组织体系、恢复流程、技术操作等内容，灾难恢复预案制定完成后应对预案设定的组织、流程和操作的可行性、正确性、有效性进行验证，并针对验证过程中出现的问题进行修正和调整。灾备中心正式启用前应至少进行一次灾难恢复演练。

6.3.7 灾备中心与生产中心的协作管理

在灾备中心交付期间应明确在日常维护期和灾难恢复期间与生产中心间的分工界面与工作流程，并对相关机制进行检验和测试，保证灾备中心投入正式运行后两中心工作协调一致。

7 灾备中心运行维护管理

7.1 日常运行维护管理

7.1.1 基础设施运维管理

灾备中心基础设施日常运维管理内容如下：

a） 基础设施监控；

b） 基础设施相关设备的维护；

c） 安防管理；

d） 卫生管理；

e） 生活设施管理；

f） 电力、通讯设施管理。

7.1.2 信息系统运维管理

信息系统日常运维管理内容和要求如下：

a） 建立灾备中心信息系统的运行监控平台，及时发现灾难备份系统运行的故障。灾备中心应保留所有监控记录，以满足故障定位、诊断及事后审计的要求；

b） 建立有效的事件跟踪机制、问题排查机制、变更管理机制，确保灾备中心的事件和问题能得到及时解决，避免重大隐患的发生；

c） 建立灾难备份系统资产清单和配置项清单，确保资产和配置项可审核、可追溯；

d） 建立灾难备份系统的定期审核与验证机制，确保灾难备份系统能够在灾难发生时接替生产系统运行。

7.2 安全管理

安全管理内容和要求如下：

a） 为灾备中心定义明确的安全管理制度，明确操作和管理权限，包括物理区域安全等级、访问授权办法，应用、数据访问途径和权限等，保证事前的控制审批和事后的审计追查；

b） 定期对灾备中心人员进行适当的安全知识及相应技能的培训，在其上岗前进行必要的资格认证并明确安全责任；对在工作中涉及组织秘密的人员（含第三方人员），签署保密协议；

c） 加强灾备中心信息资产管理，识别信息资产并建立责任制，根据信息资产重要性实施分类控制和分级保护，防范信息资产生成、使用和处置过程中的风险；

d） 建立网络通信与访问安全策略，隔离不同网络功能区域，采取与其安全级别对应的预防、监测等控制措施，防范对网络的未授权访问，保证网络通信安全；

e） 建立数据安全管理制度，规范数据的产生、获取、存储、传输、分发、备份、恢复和清理的管理，以及存储介质的台账、转储、抽检、报废和销毁的管理，保证数据的保密、真实、完整和可用；

f） 建立基础设施和重要信息的授权访问机制，制定访问控制流程，保留访问记录，防止未授权访问；

g） 建立和落实物理环境安全管理制度，明确安全区域、规范区域访问管理，减少未授权访问所造成的风险；

h） 采用适当的技术手段，包括监控、门禁、入侵检测、网络安全设备和相关信息管理平台来保证可接受的安全和效率的一致；

i） 制定紧急访问流程以保证在紧急状况发生时（如发生灾难性事件）获得效率和最基本的安全保证。

7.3 应急和切换管理

7.3.1 应急和切换

应急和切换的内容和要求如下：

a） 应建立灾难预警和预告机制，明确责任，加强与公共专业服务机构的沟通与联系，如气象、地震、消防、防疫、公安、供电等，做到灾难的早发现、早报告，提前进行灾难预防和灾难切换准备；

b） 应明确灾难恢复环境必需的资源和配置，并定期进行测试演练，以保证灾难恢复所需资源和配置的有效性。灾难恢复环境一般包括灾难备份系统的监控平台、灾难恢复指挥中心、业务恢复操作终端环境、业务连续性恢复配套资源、技术支持平台、后勤保障平台等；

c） 在灾难切换过程期间，灾备中心应在场地环境、设备操作等方面提供支持，配合将生产系统从生产中心切换到灾备中心，切换过程主要工作包括：网络切换、存储切换、主机切换、数据校验、系统校验、数据追补、业务验证等；

d） 在接替生产运营服务期间，灾备中心应加强技术支持与设施保障的资源和人力，以接替生产中心的日常工作。

7.3.2 接替生产运行

接替生产运行的内容如下：

a） 接替运行期间的灾难备份系统的维护；

b） 协助安排接替运行期间业务部门和其他单位现场工作场所和环境的保持；

c） 生产系统和灾难备份系统的切换和回退检查；

d） 协调切换和回退过程中相关人员和重要设备的转移；

e） 灾难备份系统的切换和回退后的环境清理和复原。

7.4 灾备演练管理

7.4.1 基准核对管理

基准核对管理内容和要求如下：

a） 根据灾难备份系统的范围和特点，建立灾难备份系统的基准，并形成相应的基准文档；

b） 基准文档应包括灾难备份信息系统资源的配置信息，包括主机、存储、网络、安全等硬件设备及操作系统、数据库、中间件等软件的配置信息；

c） 在灾难备份系统投入运营后，应根据变更情况，及时修改和更新基准文档；

d） 应定期（每季度至少 1 次）对生产中心和灾备中心的基准进行统计核对工作，发现差异及时处理。

7.4.2 子系统验证管理

定期（每半年至少 1 次）对各灾难备份各子系统进行能力和状态的测试工作，以保证灾难备份各子系统的有效性和运行的可靠性。

7.4.3 灾难恢复演练

灾备中心建设完成后应组织全面的演练，验证灾备中心基础设施、灾难备份系统和灾难恢复预案的正确性和有效性，进一步改进和提升灾备中心的恢复能力和管理水平。灾难恢复演练应包括演练策略的制定、演练计划的落实、演练方案设计、演练的组织、演练的实施、演练过程的过程记录和应急处置、演练结果的评估与总结。灾难恢复演练应定期（至少每年 1 次）组织，以验证灾难恢复能力。

7.4.4 预案维护

预案维护的内容和要求如下：

a） 在演练实施后，应及时进行总结，对预案进行必要的更新；

b） 应定期检查和核对灾难恢复预案中的变更情况（如成员及联络方式的变更、信息系统的日常变更等），对预案进行及时的文档更新及分发，确保预案的切实有效。