广 西 壮 族 自 治 区
数字广西建设领导小组办公室文件

桂数广办发〔2021〕38号

广西壮族自治区数字广西建设领导小组办公室关于加强壮美广西·市云灾备建设管理的指导意见

各市、县人民政府:

根据《自治区党委办公厅 自治区人民政府办公厅关于印发〈广西政务数据资源管理与应用改革实施方案〉的通知》(厅发〔2019〕141号)、《广西壮族自治区大数据发展局关于印发壮美广西·政务云管理办法的通知》(桂数发〔2020〕10号)、《广西壮族自治区数字广西建设领导小组办公室关于2020年全区非涉密数据中心和业务专网认定结果检查情况的通报》(桂数广办发〔2021〕2号),为进一步完善壮美广西·政务云灾备体系,防范化解政务信息系统安全风险,经数字广西建设领导小组同意,现提出如下

意见。

一、总体要求

（一）指导思想。

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神，进一步解放思想、改革创新、扩大开放、担当实干，加快完善壮美广西·市云体系灾备建设，构建一云承载、一网通达、一池共享、一事通办、一体安全的“五个一”政务数据治理新模式，开创政务数据资源管理与应用改革新局面，为数字广西建设提供强有力的支撑。

（二）基本原则。

1.需求导向，分步实施。以满足各级政务应用和数据备份需求为导向，壮美广西·市云灾备建设突出重点，统筹灾备中心选址、技术路线选择、业务分类分级、系统改造实施、灾备运行服务等关键环节，分步实施，确保管用实用。

2.科学求实，因地制宜。结合各地区实际，尊重产业和技术发展规律，科学论证、精准施策，正确选址灾备中心和技术路线，避免灾备中心与生产中心同时遭受影响。

3.集约整合，高效利用。充分利用现有灾备资源或社会资源，讲究实效，确保灾备资源的高效利用和有效发挥作用，提倡采用跨设区市的双中心互备建设模式或多主一备建设模式。坚持运维与建设并重，确保系统的可用性和预案的有效性。

4.技术先进，安全可控。重视引入和使用先进技术，借机实现

技术升级、系统换代和流程再造。积极运用安全可靠技术产品，推动安全与应用协调发展，筑牢平台建设和网络安全防线，确保网络和信息安全。

（三）主要目标。

到2023年，基本建成统一规范的壮美广西·市云灾备体系，全区范围内壮美广西·政务云灾备中心形成资源配置优化、布局合理、绿色集约的基础设施一体化格局；壮美广西·政务云灾备工作体系和灾难恢复工作机制基本建立；重要数据的安全性和重要业务的连续性得到有效保障，重要信息系统抵御重大技术故障风险、灾难灾害风险的能力显著提高。在此基础上，持续完善壮美广西·市云灾备体系。

二、优化灾备中心布局

（四）优化灾备中心供给结构。结合《广西壮族自治区数字广西建设领导小组关于印发〈加快构建广西一体化大数据中心协同创新体系的实施方案〉的通知》（桂数广发〔2021〕16号），全区数据中心空间布局图和配置清单，优先使用纳入布局的数据中心作为灾备中心。

（五）加强基础设施跨市共建共享。充分利用现有壮美广西·政务云网资源或社会资源，防止重复投资建设。鼓励各设区市之间加强交流合作，创新合作机制，推动数据中心等灾备基础设施的联通共用。

三、加强灾备保障能力建设

（六）推进信息系统灾备能力分类分级管理。按照国家和地方相关法规和技术标准，对壮美广西·政务云承载的信息系统和数据进行分类分级，明确信息系统的数量、业务规模、网络安全等级保护定级详情，以及各自灾备能力等级和要求，为灾备中心建设和灾备服务管理做好准备。

（七）加快灾备中心建设。根据《壮美广西·市云灾备建设技术规范》（见附件），信息系统灾备能力等级和要求，结合产生中心（云计算中心）实际，各设区市认真研究建设思路、建设模式和技术路线等，加快推进政务云灾备中心建设。对自建、服务采购等建设模式进行充分评估分析，选择适合自身的建设模式。采用自建方式，应当与通信、消防、电力、软硬件等服务商或供应商签订应急保障协议，并定期审查协议的执行情况；采用服务采购方式，应当评估外包方式的风险，制定相关的风险管控措施，履行管理责任，确保安全可控。

（八）建立健全灾备服务和运维管理体系。对灾备运行服务的内容、等级划分、注册流程以及服务申请等内容进行梳理，制定相关管理制度和业务流程规范，保障灾备业务的正常运行。建立和完善各类操作规程和管理制度，保障灾备中心的正常运转，保障备份数据及信息系统的完整性、有效性和可用性。

（九）完善灾难恢复预案，提升应急保障能力。制定并颁布灾难恢复预案，定期评估和验证灾难恢复预案的有效性，根据信息系统变更情况和演练结果不断改进完善。加强培训教育，使相

关人员了解信息系统灾难恢复的目标和流程，熟练掌握灾难恢复的操作规程。定期组织开展灾难恢复预案的演练，演练形式包括但不限于桌面演练、模拟演练、真实演练和完整演练，演练计划、过程记录和结论评估等工作文档应当保留备查。

四、强化网络数据安全管理

（十）加强网络安全管理。落实网络安全主体责任，健全考核机制。全面贯彻网络安全等级保护工作，综合运用各种网络安全防护技术手段，做好安全防护，并按照法规要求进行等级保护定级和测评。

（十一）加强数据安全管理。落实数据采集、备份、传输、存储和恢复等环节的安全责任，采取身份认证与授权管理、数据保护与审计、数据加密等技术手段实施安全保护，防范数据泄露和被非法获取，确保数据灾难备份与恢复过程的安全。

五、强化灾备建设实施保障

（十二）加强组织领导。在自治区大数据发展局的统筹指导下，由各设区市人民政府和大数据管理部门组织推进各项任务落实，切实加强组织领导，进一步细化任务、落实责任。

（十三）强化资金保障。坚持灾备体系与壮美广西·市云工程同步规划、同步建设、同步使用的原则，财政部门要统筹安排壮美广西·市云灾备体系建设和运维资金。

（十四）加强技术指导。自治区大数据发展局组织自治区信息中心和相关专家对壮美广西·市云灾备体系建设进行技术指导，

壮美广西·市云灾备建设方案应向自治区大数据发展局进行备案，自治区信息中心对壮美广西·市云灾备建设方案进行审核，出具审核意见。

（十五）强化实施落实。各设区市要切实增强紧迫感和责任感，结合实际提出落实方案，理顺本地的管理体制和工作机制，切实推动壮美广西·市云灾备建设管理工作。自治区大数据发展局要加强统筹协调、跟踪了解和督促检查，积累和推广先进经验。自治区信息中心要加强技术指导、督促检查。

附件：壮美广西·市云灾备建设技术规范

广西壮族自治区数字广西建设领导小组办公室（代）

2021年10月12日

（此件公开发布）

附件

壮美广西·市云灾备建设技术规范

一、适用范围

本规范适用于指导广西壮族自治区各设区市开展壮美广西·市云灾备规划设计、灾备体系建设和运行管理工作，主要针对灾备总体架构、建设思路、技术路线以及灾备中心的选址、备用数据处理系统、灾难恢复与演练等技术规范。

二、总体架构

灾备体系总体架构图如下所示。

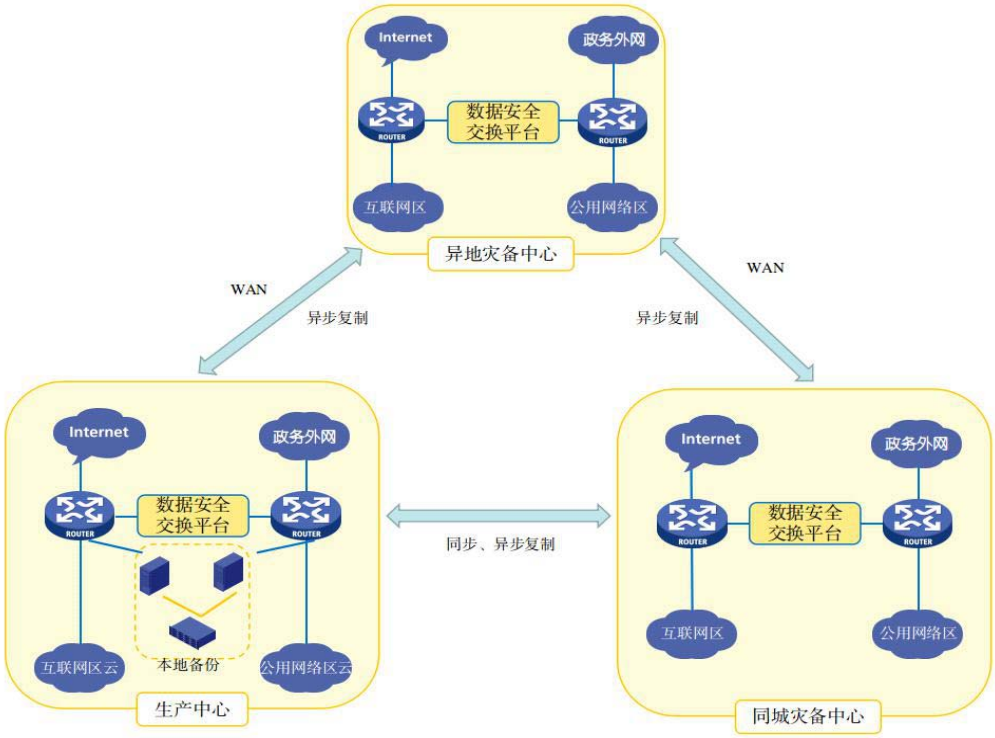

图 1　灾备体系总体架构图

采用“两地三中心”架构，在生产中心（云计算中心）基础上建设同城灾备中心和异地灾备中心。云计算中心作为生产的主中心，承载信息系统的日常运行，并具备本地数据备份能力和故障应对能力。同城灾备中心实现对生产中心实时数据的二次保护，用于防范水灾、火灾、电力中断等区域性灾难，可接管业务应用系统运行和对外提供服务，具备数据备份能力和灾难应对能力。异地灾备中心主要用于防范地震、战争等较大范围的灾难，对生产中心的数据实现远距离异地存放，并能根据需要将信息系统切换到异地灾备中心运行，具备重大灾难应对能力。

三、建设模式

（一）应用级双中心互备。

本模式适用于相互满足灾备中心选址原则，且生产云技术路线相同的（如同是华为云）两个设区市。此模式可以将己方政务云上的信息系统部署一个热备份到对方政务云上，同时保持信息系统之间的数据同步，当灾难发生时即可快速启用热备份系统，恢复业务。本地的生产系统与异地的热备份系统应处于安全隔离状态。

（二）数据级双中心互备。

本模式适用于相互满足灾备中心选址原则的两个设区市。己方可利用对方政务云的计算和存储资源，将数据备份到对方政务云上。本地的生产系统与异地的数据备份系统应处于安全隔离状态。

（三）机房级双中心互备。

本模式适用于相互满足灾备中心选址原则的两个设区市。本地可利用异地的机房机柜资源，将自有备用数据处理系统部署到异地机房，进而开展灾备系统建设。

（四）多主一备。

多个设区市共同选择一处符合各方要求地理环境优越的地点，共建灾备中心，通过集约化建设的方式降低成本和提高资源利用率。

四、总体要求

（一）合规性要求。

符合《信息安全技术 信息系统灾难恢复规范》（GB/T 20988-2007）、《信息安全技术 灾难恢复服务要求》、《信息安全技术 信息安全应急响应计划规范》（GB/T 24363-2009）和电子政务外网相关标准规范要求。

（二）专用性要求。

灾备体系涉及的支撑系统，包括机房机柜、网络、软硬件设施、运维服务体系等应为电子政务灾备体系专用。

（三）兼容性要求。

灾备体系涉及的技术体系能够兼容生产中心相关网络、操作系统、虚拟化平台、云计算平台等运行环境，能够对各种类型的应用和数据提供保护。

（四）网络安全要求。

同城灾备中心的安全防护措施应达到网络安全等级保护第三

级的要求，并按照相关法规要求向公安机关进行等保备案，且每年需通过第三级等级保护测评。

（五）数据有效性验证与灾难恢复演练要求。

应制定备份数据有效性验证和灾难恢复预案；每季度开展不少于1次备份数据有效性验证工作；每年开展不少于2次覆盖全业务范围的灾难恢复演练，模拟演练和实战演练至少各1次。

五、灾备技术路线

（一）基于备份软件的定时备份技术。本技术为传统备份技术，适用于对RPO要求不高的文件和数据库备份，可以保留多个时间点的多份备份数据，如每天备份一次，留存最近半年的备份数据。

（二）基于备份软件的持续数据保护技术（CDP技术）。基于字节级复制的CDP技术和基于块级复制的CDP技术，CDP技术的RPO接近0秒，字节级CDP技术既适用于对RPO要求高的文件和数据库备份，也适用于主机系统持续数据保护；块级CDP技术适用于主机系统持续数据保护，持续数据保护技术主要用于信息系统整机备份与恢复，一般只保留一份最新的备份数据，当需要连续保留一段时间的备份数据时成本较高。

（三）磁盘阵列异步复制技术。本技术适用于全局数据级备份，但只保留一份备份数据。

（四）磁盘阵列同步镜像技术。本技术能够保证存储层数据

实时同步，适用于构建双活应用，实现两套功能相同的应用系统在生产中心和同城灾备同时在线运行，当其中一处发生灾难时，应用系统的数据不丢失服务不中断。

（五）**数据库高可用技术**。本技术一般是关系型数据库系统自带的高可用机制，包括主备模式（Active-Standby）和主主模式（Active-Active，也称双活）。主备模式实现两套数据库系统之间异步复制数据，基本上所有的数据库系统都支持该功能；主主模式实现两套数据库系统之间实时同步数据，只有少数数据库产品支持该功能。

不同备份技术适用于不同应用场景，灾备体系需综合运用各种备份技术才能满足业务需求。双活灾备是最理想的灾备方案，其涉及基础设施、存储层、数据库层、应用层和接入访问等各个层面，是技术难度最大、成本最高的灾备方案，本规范不对双活灾备进行定义和描述。

六、灾备体系组成与技术规范

灾备建设主要包括灾备中心选址及机房配套、传输线路、数据备份系统、备用数据处理系统和备用网络与安全系统的建设。灾备中心相关备用系统与生产中心的生产系统基本一一对应，灾备体系逻辑结构如下图所示。

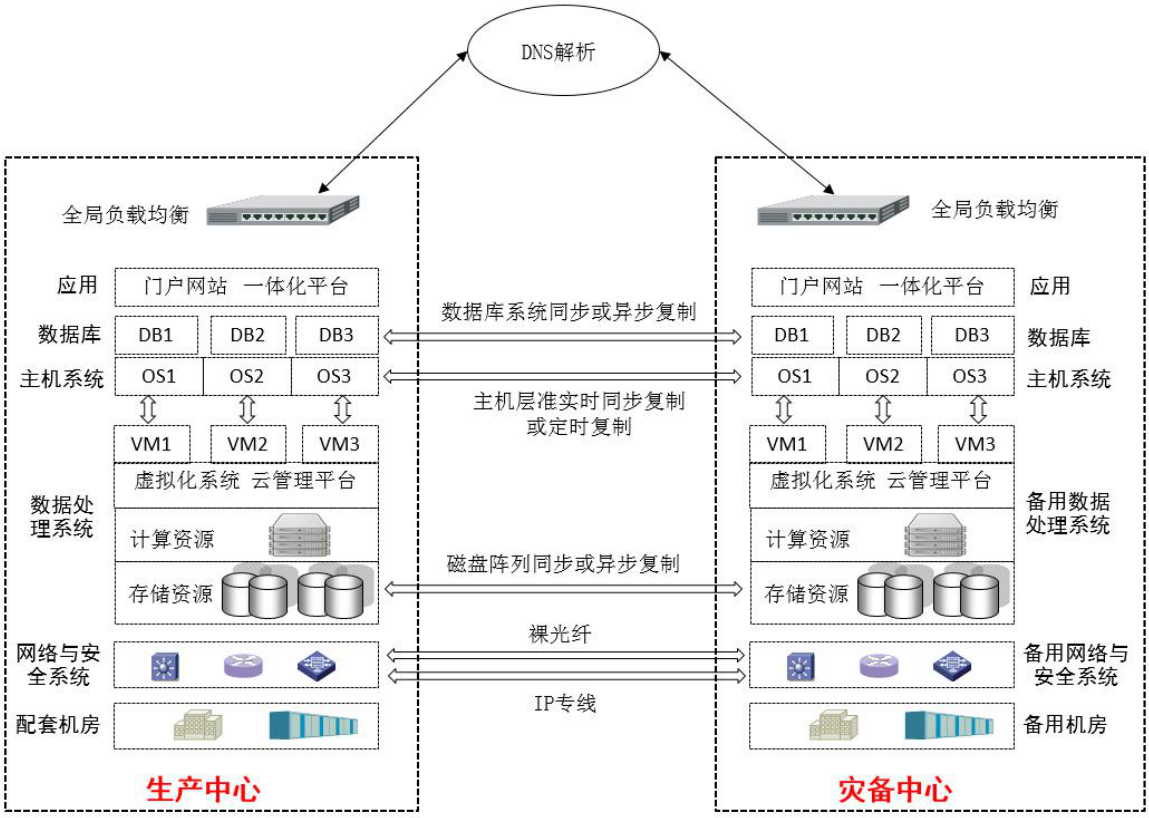

图 2　灾备体系逻辑结构

（一）灾备中心选址规范。

灾备中心选址应尽量满足以下条件：不易发生地质灾害和水涝；建筑物本身及周围没有强污染源、强放射源、强振动源、火灾易发点等安全隐患；上空无航线、附近无高速路、无高压电站、无发射电台等电磁干扰少；水源供应良好、通信条件良好；交通方便，具备较好的生活配套设施，治安安全可靠；具备充足和稳定的电力供应，且与生产中心来源于不同的电网；与生产中心不在同一地震带，不在同一江河流域。

（二）机房规范。

灾备中心机房环境原则上要求不低于生产中心。应满足以下要求：建设标准应达到中国数据中心工作组（CDCC）认证的四星级机房以上（含四星级），配备双路市电供电（需来自不同市政变电站），配备柴油发电机，UPS 系统 2N 冗余。灾备中心机房应配备动力环境集中监控系统，可以实现动力配电、场地安全、场地环境的监控需求。配备 7×24 小时全天候值班人员，并配备专业团队负责日常监控、维护、检修等工作。

（三）传输路线规范。

生产中心与同城灾备中心之间：存储系统应采用冗余裸光纤和 FC SAN 网络连接；IP 网络采用冗余的专线线路，线路带宽应能满足峰值业务需求。

本地与异地之间：应采用冗余的专用数字电路，端到端时延≤20ms，且冗余的专线为不同路由线路，线路带宽应能满足峰值业务需求。

（四）数据备份系统规范。

数据备份系统是灾备体系的核心功能组件，用于实现数据备份和恢复。数据备份系统的建设首先要确立信息系统的灾备能力等级，然后根据灾备能力要求选择合适的技术路线，最后综合运用各种技术路线设计数据备份系统。一套数据备份系统（软件）可以覆盖生产中心、同城灾备中心和异地灾备中心共同使用。

（五）备用数据处理系统规范。

备用数据处理系统用于承载备份软件的运行和信息系统故障

或灾难恢复，主要包括计算资源、存储资源和云计算管理平台（或虚拟化平台），需要在生产中心和同城灾备中心建立备用数据处理系统。备用数据处理系统应对应生产中心的架构，分设互联网区和公用网络区并各配置一套备用数据处理系统。

1.生产中心的备用数据处理系统。

生产中心的备用数据处理系统主要用于故障恢复，其使用频率较高，同时发生故障的信息系统数量不多，配置的备用数据处理系统应功能齐全、规模较小，存储资源需充足。原则上配置的计算资源、存储资源和云计算管理平台（或虚拟化平台）与生产中心的保持一致更有利于数据迁移和故障恢复。

2.同城灾备中心的备用数据处理系统。

同城灾备中心的备用数据处理系统主要用于应对一般的灾难，使用频率较低，一旦启用使用要求则很高，需要根据实际需求配齐计算资源、存储资源和云计算管理平台（或虚拟化平台），其资源与生产中心的保持一致更有利于灾难恢复。

3.异地灾备中心的备用数据处理系统。

配置用于支撑数据备份系统运行所需的计算和存储资源即可，或参照本文件的建设思路根据实际情况配置。

（六）备用网络与安全系统规范。

1.生产中心的备用网络与安全系统。

对应生产中心的互联网区和公用网络区架构，分别建设独立的备份网络区域，并将备份网络区域接入生产中心的骨干网。备

份网络区域利旧使用生产中心的互联网出口、政务外网出口、以及相关安全设施。

2.同城灾备中心的备用网络与安全系统。

对应生产中心的网络架构，建设完备的数据中心局域网。网络区域设置应包括互联网接入区和互联网业务区、数据安全交换区、政务外网接入区和公用业务区等。网络接入带宽应不小于千兆，骨干网带宽应不小于万兆。原则上同城灾备中心与生产中心应处在同个大二层网络下，以支持应用集群跨数据中心部署和同步数据，支持虚拟机备份资源能够快速恢复，配套的网络安全防护措施应能达到三级等保要求。

3.异地灾备中心的备用网络与安全系统。

主要用于支撑数据级备份，应分设逻辑隔离的互联网区和公用网络区用于接入和运行数据备份系统，或参照本文件的建设思路根据实际情况配置。

广西壮族自治区数字广西建设领导小组办公室　2021年10月22日印发