灾 备 技 术 产 业 联 盟 标 准

T/ ZBLM 0001—2023

电子政务云灾备体系建设规范

Specifications for the Construction of E-government Cloud Disaster Recovery System

2023 -08-14 发布　　2023- 09 -14 实施

北京信息灾备技术产业联盟　　发 布

目　录

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。

本标准由北京信息灾备技术产业联盟提出并归口。

本标准主要起草单位：灾备技术国家工程研究中心、中国信息通信研究院、北京市政务信息安全保障中心、北方工业大学、山东省大数据局、山东省大数据中心、山东省烟台市大数据中心、山东省枣庄市大数据中心、山东省潍坊市大数据中心、重庆市大数据应用发展管理局、重庆市綦江区大数据应用发展管理局、上海数腾软件科技股份有限公司、成都云祺科技有限公司、深圳大普微电子科技有限公司、四川精容数安科技有限公司、飞创信息科技有限公司、柏科数据技术（深圳）股份有限公司、上海爱数信息技术股份有限公司、北京中嘉和信通信技术有限公司、深圳市德弊数据有限公司、睿至科技集团有限公司、中电云计算技术有限公司、上海英方软件股份有限公司、北京国腾创新科技有限公司、平安科技(深圳)有限公司

本标准主要起草人：辛阳、李芳、于铮、张治兵、马礼、杨光灿、刘欣东、刘雅闻、魏淑斌、张荣光、李鲁、王少煜、白秀军、朱少伟、李志臣、黄星华、黄洁、徐礼长、黄传波、杨亚飞、康乐、庞力荣、游录金、汪惠春、梁军海、冯凯、刘凤屿、王丽红、胡华璐、李文莉

电子政务云灾备体系建设规范

1 范围

本文件规定了电子政务云灾备安全保障管理、灾备技术、应急预案与灾难恢复演练及灾备系统分类分级应遵循的基本要求。

本文件适用于电子政务云管理单位和资源使用单位，用于指导电子政务云灾备建设、管理和运维。

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 22239-2019　信息安全技术 网络安全等级保护基本要求

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

GB/T 31167-2014　信息安全技术 云计算服务安全指南

GB/T 31168-2014　信息安全技术 云计算服务安全能力要求

GW0013-2017　国家电子政务外网标准：电子政务云安全要求

C 0116-2018　国家政务服务平台网络安全保障要求

C 0117-2018　全国一体化在线政务服务平台应急保障要求

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1 缩略语

RTO：恢复时间目标（Recovery Time Objective）

RPO：恢复点目标（Recovery Point Objective）

DOO：降低运行目标（Degraded Operations Objective）

NRO：网络恢复目标(Network Recovery Objective)

APIT：任意时间点回退 (Any Point In Time)

BIA：业务影响分析（Business Impact Analysis）

3.2 术语

3.2.1 电子政务云灾备系统 government cloud disaster recovery system

用于电子政务云灾难恢复目的，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，以满足电子政务云业务运行的连续性要求。

3.2.2 分析评定时间点 analysis and evaluation time point

对电子政务云系统进行灾备分类级别评价的时间。

3.2.3 检视再分析周期 review reanalysis cycle

当受保护的电子政务云应用系统发生重大变化时，对电子政务云灾备系统重新检查、分析和定义灾备级别的时间周期。

3.2.4 风险分析 risk analysis

风险分析指依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息/数据的保密性、完整性和可用性等安全属性进行评价的过程。评估信息资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的信息资产价值来判断安全事件一旦发生对组织造成的影响。

3.2.5 任意时间点回退 any point in time

是指在数据发生逻辑错误时，对破坏的数据进行恢复，这时持续数据保护技术的衡量标准可以用任意时间点回退进行评判。

3.2.6 BIA 业务影响分析 business impact analysis

是指确定IT系统中断可能对业务造成的影响，得出容灾指标（RTO和RPO）的过程。

3.2.7 恢复时间目标 recovery time objective

是指灾难发生后，从系统宕机导致业务停顿之刻开始，到系统恢复至可以支持业务部门运作，业务恢复运营之时，此两点之间的时间。

3.2.8 **恢复点目标** recovery point objective

是指灾难发生后，灾备系统能把数据恢复到灾难发生前时间点的数据，是衡量系统在灾难发生后会丢失多少生产数据的指标。

3.2.9 **降低运行目标** degraded operations objective

是指灾难事件发生期间数据中心不可用时，关键业务系统在灾备中心运行的服务级别允许降低到一个可接受程度。

3.2.10 **网络恢复目标** network recovery objective

是指在灾难发生后切换到灾备中心所需的时间。

3.2.11 **灾难恢复演练** disaster recovery exercises

验证电子政务云灾难备份系统的有效性，确保电子政务云灾难备份系统能够有效接替生产系统运行，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。

注：灾难恢复演练的形式可以分为桌面演练、模拟切换演练和实战演练。

4 电子政务云系统灾备评估要求

4.1 风险分析

风险分析的目标为电子政务云灾备系统，评估内容应包括机房场地、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，通过识别潜在的安全风险隐患、系统漏洞、系统固有脆弱性，制定防范或控制风险的可行性方案，采取相应的风险管控措施，提高风险抵御能力。风险分析方法应依据GB/T 20984所要求的内容开展。

电子政务云灾备主管部门应每年进行一次风险分析评估工作，通过风险评估分析，发现安全风险、采取控制措施、完善组织的安全管理体系。

4.2 分析评定

电子政务云系统迁移到云平台之后或者新部署的应用系统，应评定电子政务云系统灾备级别。在电子政务云灾备系统运行一年后，应分析评估电子政务云灾备系统是否满足分类级别要求。

当电子政务云系统核心业务流程、系统架构、生产环境发生重大变更时，应在三个月内对电子政务云应用系统进行业务影响分析，开展灾备级别检视再分析，重新定义灾备级别，制定电子政务云系统灾备策略和计划。

4.3 业务影响分析

（1）业务核心功能分析

应对电子政务云系统各项业务功能之间的相关性进行分析，确定支持各种业务功能的相应应用系统资源及其他资源，明确相关信息的保密性、完整性和可用性要求。

（2）依赖性分析

应对电子政务云系统的应用架构、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。

（3）业务中断影响分析

应采用定量分析和定性分析的方法，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中5.2.2节。

5 电子政务云系统灾备分类分级

5.1 系统重要性分类

电子政务云业务运维主管部门应分析业务核心功能中断影响，结合系统间的依赖性，确定应用系统的重要程度。根据风险分析、业务影响分析的结论，将电子政务云部署的支持关键业务重要性分成五种类别，详见附录A.1。

政务类系统重要等级分析维度包括不限于：政务机构业务范围、社会影响、机构财政影响、人员影响的程度。RTO对应应用系统不可用的时间长度造成的影响程度，RPO对应系统数据丢失量造成的影响程度。

业务运维主管部门，通过系统重要等级分类，确认应用系统关键级别、判断业务的连续性要求、分析各级别对应的RTO和RPO，以便制定对应的连续性保障策略，详见附录A.2。

5.2 灾难恢复能力分级

根据风险分析的结论，按照灾难恢复资源的成本与风险可能造成损失之间的平衡原则确定关键业务功能的灾难恢复策略，不同的业务功能采用不同的灾难恢复策略。灾难恢复策略应包含灾难恢复能力等级，等级依据GB/T 20988附录A中第2级至第6级的等级进行划分。电子政务云系统灾难恢复能力等级与RTO/RPO对应关系见附录B.1。

根据电子政务云灾难恢复能力等级的RPO、RTO指标，电子政务云系统对应的业务连续性指标要求见附录表B.2。

6 电子政务云灾备方案制定

在设计电子政务云灾备系统时，应根据各个业务系统的重要性和业务连续性要求的不同，对各业务系统进行优先级排序，确定电子政务云系统恢复优先级，并制定不同的灾备方案。

表1 可选灾备方案表

所有业务系统中的优先级	可选灾备方案
五级	1、业务连续性和数据实时复制 2、远程完整灾备系统 3、业务自动切换到灾备端 4、需要业务端定制开发
四级	1、业务热备和数据实时复制 2、远程完整灾备系统 3、业务自动/手动切换到灾备端 4、需要业务端定制开发
三级	1、业务冷备和数据库复制/CDP 连续数据保护 2、远程完整灾备系统 3、业务手动切换到灾备端
二级	1、定时本地备份和远程备份 2、从远程灾备系统直接恢复到业务系统
一级	定时本地备份+远程备份

7 技术要求

电子政务云灾备在建设时，使用方、建设方和设计方应进行充分论证和评估确定满足符合对应级别的技术要求。

7.1 总体要求

（1）选用电子的政务云灾备系统应支持云容灾部署能力；根据实际需求部署灾备方式，应提供同城和异地两种备份容灾部署方式，同城灾备中心系统在同一城市的不同地址，距离主数据中心距离在50公里以内；异地灾备中心系统应在不同城市，距离主数据中心200公里以上，做数据级或应用级容灾备份；

（2）选用电子的政务云灾备系统应提供实时和定时数据备份能力；

（3）选用电子的政务云灾备系统应具备等同生产环境业务处理能力的网络链路；

（4）选用电子的政务云灾备系统应保证灾备系统管理数据（如索引文件、云服务客户信息及密钥等）、鉴别信息和重要业务数据（如用户隐私数据）存储和传输的完整性和保密性；

（5）应能针对电子政务云灾备系统内不同权限人员的存储数据进行隔离，防止电子政务云灾备系统不同用户间非授权访问敏感数据；

（6）重要数据应采取密码机制保护措施，密钥的生成、存储、使用和管理应符合相关国家标准和国家密码管理局关于商用密码的管理要求；

（7）应满足数据恢复和重建目标的需求。通过确定备份时间、技术、介质和场外存放方式，以保证达到RPO和RTO的要求，具体标准应通过云服务方，云用户和云管理单位三方确定；

（8）正式上线前应进行测试，并向电子政务云用户方提供第三方机构检测报告备案。

7.2 电子政务云灾备中心选址要求

（1）应提供充足可靠的电力供给，保证通信快速畅通；对同城灾备的选址不应在同一个变电站，且不应在同一个通信局间；

（2）如采用水蒸发冷却方式制冷的数据中心机房，水源应供应充足；

（3）应远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆等物

品的场所；

（4）应远离水灾、泄洪区、地震、台风、低洼易涝等自然灾害隐患区域；

（5）应远离强振动源、强噪音源、强电磁场、核辐射源等区域。

7.3 物理平台要求

（1）灾备机房应安排专人值守，配置门禁系统，控制和记录进出机房人员；

（2）应将灾备系统设备或主要部件固定，防止盗抢；

（3）应将灾备系统各类机柜、设施和设备等通过接地系统安全接地；

（4）灾备机房应安装灭火设施；

（5）灾备机房应具备防漏雨、漏水等有效措施；

（6）灾备机房环境应保持清洁，环境温度应保持在设备允许运行的范围之内，且有利于节约能源。

7.4 网络要求

（1）同城灾备中心和异地灾备中心网络均应采用不同运营商的双链路模式，单链路带宽均应不低于500Mb/s；

（2）不同用户客户端到电子政务云灾备系统之间的远程数据传输应采取保护和隔离措施；

（3）应提供网络访问控制使云灾备服务客户实现网络分段和隔离，包括网络过滤功能；

（4）应具备防火墙策略迁移的能力，当业务切换到灾备系统时，可以方便灾备云服务客户违规行为能够被及时阻断、清除安全威胁；

（5）应具备与生产系统相同的安全防护能力，部署相应设备防范互联网的各类攻击。

7.5 功能要求

7.5.1 灾备部署

（1）选用的电子政务云灾备系统应支持部署到物理服务器和虚拟化平台；

（2）选用电子的政务云灾备系统应支持备份软件、备份主机、备份介质一体化部署模式；

（3）选用电子的政务云灾备系统应支持双中心和多中心部署模式。

7.5.2 数据备份恢复

（1）应支持根据数据分类标准进行数据的本地、同城或异地的备份；

（2）应支持对文件或目录、数据库、存储块数据及操作系统进行备份恢复；

（3）应支持完全备份、累积增量备份和差分增量备份，并能够根据备份对象、备份介质、备份时间、备份方式、备份数据保存时间等条件制定备份策略。

（4）应支持利用备份数据进行数据完整性、可用性的验证。

7.5.3 数据库复制

（1）应支持数据库实时同步复制功能，实时将数据库备份到目标端，目标端数据库实时可读；

（2）应支持国内外主流数据库应用；

（3）应支持不同的数据库复制模式；

（4）应支持所有数据库对象、所有数据类型（包括用户自定义类型）的复制；

（5）应支持以邮件或短信的方式实时提醒数据库复制状态及告警。

7.5.4 数据恢复演练

（1）应支持备份数据的自动恢复演练功能，通过创建自动恢复演练策略，定时将已备份的数据自动恢复到指定位置；

（2）应支持主流应用数据类型；

（3）应支持自定义恢复演练目标客户端和恢复路径；

（4）应支持不高于24小时为周期配置自动演练策略；

（5）应支持配置精确到分钟级的演练执行时间策略。

7.5.5 灾备切换

（1）应确保生产端和灾备端网络的通畅，支持网络和应用层的切换；

（2）应通过脚本或其他方式设定切换阀值，利用心跳线判断达到切换的条件；

（3）应明确需要切换的应用系统的顺序，通过手动或自动的方式进行切换；

（4）应支持反向的灾备切换，确保源端恢复正常运行后，可接管备端的生产业务继续运行；

（5）应支持主机级和系统级的自动切换及手动切换功能，保证生产系统在灾备切换过程中的灵活性；

（6）应提供主备系统之间的相互切换功能；

（7）应提供灾备演练功能。

7.5.6 应用迁移安全

（1）应支持电子政务云应用迁移一致性校验功能；

（2）应支持电子政务云应用业务任意时间点恢复功能；

（3）应采取措施保证电子政务云应用迁移过程中的数据安全；

（4）应用迁移应保证不影响和不篡改源端应用的原则下进行；

（5）应用迁移不应破坏源端应用的用户管理、密码管理、加密管理和安全体系；

（6）应用迁移不应另行增加超级用户进行侵权操作；

（7）应支持应用迁移过程中的传输数据加密；

（8）应支持应用迁移产生副本数据纳入统一安全监管平台，进行合理使用；

（9）应用迁移完成后，应提供完整的迁移工作报告；

（10）应用迁移产生的缓存数据，应在迁移完成后统一清除销毁；

（11）应用迁移过程中发现影响源端应用、数据泄漏和其他安全隐患，应支持停止迁移任务。

7.5.7 云存储安全

（1）应支持数据云加密存储，保证从网络到存储层面数据的安全性；

（2）应采取有效的访问控制策略，保证访问及对关键数据操作获得有效授权；

（3）应支持在云灾备系统数据存储的数据完整性进行保护；

（4）应支持对云存储上的用户敏感信息进行数据保护；

（5）应支持不可变云存储技术，应对黑客和勒索病毒攻击；

（6）应支持强制数据保留能力，对于关键数据不能通过任何方法进行删除和修改。

7.5.8 重复数据删除

（1）应支持重复数据删除功能，避免存储资源过度占用；

（2）重复数据删除产生的指纹库应有相应的安全措施进行保护；

（3）应支持内存级重复数据删除。

7.5.9 身份认证与授权安全

（1）应具备用户身份认证功能，认证方式不限于用户名/口令、Ukey认证、生物认证等；

（2）应对用户身份进行标识和鉴别，用户标识应具有唯一性；

（3）应对用户身份鉴别信息进行安全保护，保障用户鉴别信息存储和传输过程中的保密性；

（4）应支持访问控制功能，只有使用指定的IP登录才可以对系统执行管理操作以及业务的访问；

（5）应提供登录失败处理功能，包括但不限于限制连续的非授权登录尝试次数等；

（6）应提供登录超时锁定或退出、会话锁定功能，在重新管理备份系统时需再次进行身份鉴别；

（7）在采用基于口令的身份鉴别时，应对用户设置的口令进行复杂度检查，确保用户口令满足一定的复杂度要求；

（8）当产品中存在默认口令时，应在用户首次登录时提示用户对默认口令进行修改。

7.5.10 数据通信传输安全

（1）在数据备份和恢复时，应采取措施保证数据通信传输过程中的安全；

（2）灾备数据通信传输过程中，应有保护措施，不得明文传输用户敏感信息（如口令等）和灾备数据内容信息；

（3）应设置数据通信传输（远程复制）的窗口期，避免非传输时段灾备服务对外暴露造成的安全隐患。

7.5.11 安全审计

（1）应提供日志审计功能，对用户关键操作行为和重要安全事件（如登录、备份和恢复等操作）进行记录，应支持对影响设备运行安全的时间进行告警提示；

（2）应支持对备份对象，备份策略，重要参数的日志审计；

（3）日志审计应记录必要的要素，主要包括：发生的时间日期、事件主体、客体身份和事件描述等要素；

（4）应提供对日志查看和存储进行保护的功能，防止日志被未授权者查看或删除；

（5）日志存储时间应不少于6个月。

7.5.12 数据存储要求

（1）应对存储在电子政务云灾备系统中的敏感数据进行加密保护；

（2）应对关键业务中的鉴别信息、重要业务数据进行加密存储。

7.5.13 数据同步要求

（1）应支持卷、文件、虚拟机和数据库实时同步功能；

（2）数据完成同步后，生产中心与灾备中心的数据应保持一致。

7.5.14 高可用要求

（1）应支持高可用集群架构，每个灾备节点均可作灾备服务的负载节点；

（2）应支持通过负载均衡系统代理转发、均衡分配资源，保证瞬间高并发的灾备请求分配到不同节点上的存储服务和重复删除服务；

（3）单中心部署时应支持主备模式，确保实现系统宕机无法继续提供服务时，可通过启动备用灾备系统进行接管，恢复生产业务；

（4）应确保备用灾备系统可正常启动运行。

7.5.15 服务模式要求

（1）应支持IaaS、PaaS、SaaS服务模式下的灾难备份与恢复功能；

（2）灾备系统应提供标准API接口，供云管理平台和监控审计平台的数据调用。

7.5.16 扩展性要求

应支持存储资源、备份容量和备份节点扩展，保证在系统运行中具备足够的备份资源，且在扩展后不影响已有备份数据。

7.5.17 可视化要求

（1）应支持图像化展示备份系统各模块的整体运行情况，包括虚拟机、文件、数据库、操作系统等；

（2）应支持展示监控状态信息、数据统计、故障报警等；

（3）应支持呈现灾备任务状况和汇总的可视化界面；

（4）应支持呈现灾备系统存储视图的可视化界面；

（5）应呈现灾备任务故障、灾备网络故障和灾备存储故障等异常事件的可视化界面。

7.6 性能要求

7.6.1 文件备份性能

（1）单链路网络带宽下（500Mb/s），小文件（≤4KB）备份速度不低于20MB/秒；

（2）单链路网络带宽下（500Mb/s），大文件（≥4MB）备份速度不低于40MB/秒。

7.6.2 文件恢复性能

（1）单链路网络带宽下（500Mb/s），小文件（≤4KB）恢复速度不低于10MB/秒；

（2）单链路网络带宽下（500Mb/s），大文件（≥4MB）恢复速度不低于40MB/秒。

7.6.3 操作系统备份恢复性能

（1）单链路网络带宽下（500Mb/s），操作系统备份平均速度不低于20MB/秒；

（2）单链路网络带宽下（500Mb/s），操作系统恢复平均速度不低于40MB/秒。

7.6.4 数据库备份恢复性能

（1）单链路网络带宽下（500Mb/s），数据库备份速度不低于40MB/秒；

（2）单链路网络带宽下（500Mb/s），数据库恢复速度不低于30MB/秒。

7.6.5 虚拟机备份恢复性能

单链路网络带宽下（500Mb/s），虚拟机备份和恢复速度均不低于40MB/秒。

8 安全保障管理要求

8.1 保障管理要求

（1）保障管理组织机构

1）应成立电子政务云灾备安全保障领导小组（以下简称领导小组），其组长应由各级电子政务云系统主管单位的主要负责人担任，领导小组组长作为电子政务云系统灾备安全第一责任人，承担领导和管理责任；

2）灾备系统与生产系统应统一安全保障管理团队，应设立系统管理员、网络管理员、安全管理员等岗位，并明确各个工作岗位的职责；

3）应设立应急响应团队，负责电子政务云系统灾备应急响应工作，应急响应团队应在领导小组的领导下开展工作，负责应急响应工作的具体执行。

（2）安全管理制度

灾备系统的安全管理等级与要求应与生产系统保持一致，并与生产系统的安全管理要求同步建设和更新。灾备系统安全管理制度应包括但不限于：

1）建立安全应急保障机制，制定安全事件日常监测和应急处置流程，有效预防和应对安全事件的发生；

2）建立安全评估与审计机制，对灾备系统的安全状况进行深入全面完整的评估和审计，及时发现安全体系存在的问题和漏洞；

3）安全自查与演练机制，定期组织灾备系统安全自查工作，并组织对安全事件应急预案及处置措施进行实战演练，持续保持各项安全措施的完整有效，不断优化和完善应急预案，应急预案和灾难恢复演练参见附录C要求；

4）应制定完备的信息安全保密制度并严格执行。针对重要数据的使用、传递和保存应制定严格的管理制度，防止重要信息外泄；

5）应定期（至少每半年一次）组织灾备安全管理人员进行安全知识和技能培训，并通过考核机制保证培训效果。

8.2 技术管理要求

电子政务云灾备系统要满足电子政务云信息资源的保密性、完整性和可用性要求。电子政务云灾备系统安全保障技术要求包括但不限于：

（1）网络隔离要求

对于多个生产系统共享的灾备系统，建设时应对不同生产系统的通信进行安全隔离，避免由于多个生产系统在灾备系统内部的通信互通导致的安全隐患。

（2）存储安全要求

1）应根据有承载数据业务的安全需求，制定合理的存储策略，不同安全级别的数据应存放在不同的存储空间中；

2）存储设备应提供完整数据访问权限控制；

3）存储设备应提供实时的安全监控。

（3）数据安全要求

1）应采用加密或其他有效措施实现备份系统管理数据、重要业务数据、鉴别信息等在传输过程中的保密性；

2）应能够检测到备份的系统管理数据、重要业务数据、鉴别信息在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要恢复措施；

3）备份的系统管理数据、重要业务数据、鉴别信息等应加密存储；

4）备份数据保存期限应符合电子政务云数据存储相关规定要求；

5）应对备份政务数据进行分类管理，不同类别的政务数据应采取不同的安全保护措施。具体数据分类和保护措施参见标准C 0116-2018附录A。

8.3 运行和维护要求

（1）运行和维护管理要求

电子政务云灾备系统运行维护管理要求应关联生产系统的运维管理体系，在日常管理流程、人员岗位构成、演练组织等方面应与生产系统关联。灾备系统运行维护管理内容包括但不限于：

1）应建立灾备系统的运行监控能力，及时发现灾备系统运行的故障，应保留监控记录以满足故障定位、诊断及事后审计的要求；

2）应建立灾备系统的资产清单和配置项清单，确保资产和配置项的可审核、可追溯；

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

4）应建立数据备份与恢复管理制度，根据数据的重要性和对系统运行的影响程度，制定数据的备份策略和恢复策略；

5）应对数据的备份方式、备份额度、存储介质和保存期限进行规定；

6）应建立控制数据备份和恢复过程的程序，记录备份过程，保证数据安全，避免数据泄露、遗失；

7）应制定相应的灾难恢复计划，形成灾难恢复预案，定期进行测试、演练，以确保各个恢复环节的正确性和计划整体的有效性，内容包括数据恢复、运行系统恢复、备用系统接管等。

（2）运维人员岗位职责

电子政务云灾备系统与生产系统由上级组建维护管理团队，设定专人负责灾备系统的运行管理，岗位职责包括但不限于：

1）负责灾备系统的监控及日常操作；

2）负责灾备系统的专业技术支持；

3）负责运行事件、问题的处理和管理；

4）负责灾备系统资源变更管理；

5）负责灾备系统及数据有效性和完整性的验证；

6）负责灾难恢复预案的维护和管理；

7）负责灾难恢复演练。

附录

附录 A 系统重要性等级分类表

A.1 重要等级分类表

表A.1给出了电子政务云系统重要等级分类。

附A表1 重要等级分类表

重要等级分类	分类描述
第一类	涉及国家安全、社会秩序、经济建设和公共利益的核心政务系统。应用系统短时间中断或数据丢失会对社会秩序、经济建设和公共利益造成严重影响，对政务机构履行其政务职能、机构财产、人员造成极其严重的负面影响。
第二类	涉及国家安全、社会秩序、经济建设和公共利益的重要政务系统。应用系统短时间中断或数据丢失会对社会秩序、经济建设和公共利益造成较大影响，对公民、法人和其他组织的合法权益造成较大影响，对政务机构履行其政务职能、机构财产、人员造成严重的负面影响。
第三类	涉及处理重要政务信息和提供重要政务服务的政务系统。应用系统中断会造成政务中断或数据丢失，影响政府部门日常工作、组织的日常经营运转、公民日常生活，对政务机构履行其政务职能、机构财产、机构形象和信誉造成较大的负面影响。
第四类	用于处理日常政务信息和提供一般政务服务的电子政务系统。系统中断后对政务机构履行其政务职能、机构财产、机构形象和信誉造成中等程度的负面影响。
第五类	用于一般的电子政务系统。系统遭到破坏后对政务机构履行其政务职能、机构财产、机构形象和信誉造成较小的负面影响。

A.2 重要等级分类标准与 RTO 和 RPO 对应关系表

表A.2说明了电子政务云系统重要等级分类标准与RTO和RPO对应关系。

附A表2 重要等级分类标准表

关键类别	重要性	标　　准	RTO	RPO
一类	关键	应用系统短时间中断或数据丢失，会对社会秩序、经济建设和公共利益造成严重影响，对政务机构履行其政务职能、机构财产、人员造成极其严重的负面影响。有严格的制度约束和法律责任。	<=15分钟	0分钟
		系统中断将导致中央政务机构的一项或多项政务职能无法履行。影响到省级以上各层政务机构日常运作，或面向省级及以上公众范围提供服务。		
		存在长期性的财政、民生影响。		
		没有业务应急处理方案或应急处理方案实施难度大，准备时间长。		
二类	重要	应用系统短时间中断或数据丢失会对社会秩序、经济建设和公共利益造成较大影响，对公民、法人和其他组织的合法权益造成较大影响，对政务机构履行其政务职能、机构财产、人员造成严重的负面影响。	<=1小时	≈0分钟
		系统中断将导致省级政务机构的多项政务职能无法履行，影响政务机构日常运作，或面向市级及以上公众范围提供服务。		
		对政务机构、相关单位、人员有严重的财政影响，经济损失。		
		有短期的应急业务处理方案。		
三类	较重要	应用系统中断会造成政务中断或数据丢失，影响政府部门	<=4小	<=1小

		日常工作、组织的日常经营运转、公民日常生活，对政务机构履行其政务职能、机构财产、机构形象和信誉造成较大的负面影响。	时	时
		间接支持关键政务业务功能，政务机构对系统短时间中断有一定的容忍度。对政务机构运行带来较大的负面影响，政务机构的一项或多项政务职能无法履行，影响到多个部门。		
		对政务机构、相关单位、人员有一定的经济损失，或对形象或名誉造成较大的负面影响。		
		有短期的应急业务处理方案。		
四类	一般	系统中断后对政务机构履行其政务职能、机构财产、机构形象和信誉造成中等程度的负面影响。	<=24小时	<=24小时
		支持一般政务业务，而且在主数据中心完全恢复之前不用运行。仅影响单政务机构，应用不可用对日常政务运转存在一定的影响，效率较大程度降低，不向公众直接提供服务。		
		对政务机构、单位、个人有一定的形象和名誉上的影响。		
		有长期的备用业务处理方案。		
五类	次要	系统遭到破坏后对政务机构履行其政务职能、机构形象和信誉造成较小的负面影响。	<=7天	<=36小时
		对于日常政务不是必需的，而且在数据中心完全恢复之前不用运行。仅影响本政务机构，政务机构可以继续履行其基本的政务职能，但效率有较小程度的降低，不向公众直接提供服务。		
		对政务机构、单位、个人很少或者根本没有财政、名誉上影响。		
		不影响日常政务业务功能，有长期替代业务处理方案。		

附录 B 灾难恢复能力等级

B.1 电子政务云灾难恢复能力等级与 RTO/RPO 对应关系表

表B.1说明电子政务云灾难恢复能力各等级与RTO/RPO对应关系。

灾难恢复等级	GB/T 20988对应级别	RTO	RPO
第一级	第2级	RTO≤7天	RPO≤36小时
第二级	第3级	RTO≤24小时	RPO≤24小时
第三级	第4级	RTO≤4小时	RPO≤1小时
第四级	第5级	RTO≤1小时	RPO≤1分钟
第五级	第6级	RTO≤15分钟	RPO=0秒钟

B.2 电子政务云系统对应的业务连续性指标

表B.2说明电子政务云对应的业务连续性指标。

电子政务云灾难恢复等级	DOO	NRO	APIT
第一级	50%	≤7天	天级
第二级	70%	≤24天	小时级
第三级	80%	≤4小时	分钟级
第四级	90%	≤1小时	秒级
第五级	100%	≤15分钟	毫秒级

附录 C 应急预案与灾难恢复演练

（1）总体应急预案

应制定电子政务云灾备总体应急预案。总体应急预案是电子政务云运营机构对运营中断事件的总体方案，包括总体组织架构、各层级预案的定位和衔接关系以及对运营中断事件的预警、报告、分析、决策、处理、恢复等处置程序。同时应根据事故危害程度、影响范围、损失等明确划分事件等级。总体预案宜用于处置导致大范围业务运营中断的事件。

（2）业务专项应急预案

应制定电子政务云重要业务专项应急预案，专项应急预案应注重灾难场景的设计，明确在不同场景下的应急流程和措施。业务专项应急预案包括：

1）事件发生的场景、范围、恢复时间目标和恢复点目标；

2）应急事件初始响应、危害和重要性评估；

3）指挥中心应急启动的决策及授权；

4）应急事件处理过程中涉及的部门和人员，联络方式和各自的职责；

5）应急处理技术方案和操作手册；应急处理过程中需要的资源；

6）应根据应急事件等级的要求制定并实施相应的应处理预案，内容应明确应急响应的目标、原则、范围以及各项保障措施，并定期评审。

（3）教育和培训

应定期组织应急预案的教育和培训，确保相关人员熟知预案，培训后应保留培训记录。通过演练验证应急预案的可行性，促进相关人员掌握应急预案中所规定的职责和程序，检验指挥决策和协同配合能力，提高指挥、运维和保障人员应急处置的能力。

（4）应急灾难恢复演练管理

应制定应急灾难恢复演练管理方案。方案应包括应急演练计划、实施应急演练、应急演练后评价以及应急预案的持续改进，通过演练训练指挥人员和运维人员掌握和提高应急处置的能力。在重大业务活动、重大社会活动等关键节点，或在关键资源发生重大变化之前，应当开展电子政务云灾备系统的专项演练。

1）应急演练按照演练形式分为桌面演练、模拟演练、实战演练。桌面演练是组织相关人员，以会议形式模拟各种应急场景，集中讨论应急响应和恢复流程中的管理与指挥协

调，验证应急预案是否满足要求；模拟演练是模拟应急场景，利用备份系统实施应急预案模拟操作。模拟演练不应影响系统的正常运行；实战演练是模拟真实场景，对正在运行系统人为制造故障，按照应急预案完成系统切换或业务恢复，在演练完成后需进行系统的回切和恢复。

在进行真实演练前应当事先对备份资源进行技术验证，确保其可用性；在实施灾难备份切换演练时，应对备份系统的运行情况实施监控。

2）桌面演练和模拟演练应覆盖所有的应急预案，对基础设施重要系统的实战应急演练每年应不少于一次，实战演练宜每三年覆盖所有应急预案的场景。应全面记录演练过程，形成演练报告，提出改进意见。演练完成后，需要对演练的组织、过程、效果进行评估，演练的评估内容包括：应急预案的有效性和可用性；演练结果与演练目标的差距；演练过程中发现的问题；演练工作的组织；参演人员的应急能力；应急资源的协调和保障能力；形成应急演练的总结报告；提出改进意见和完善应急预案。

3）应每年进行一次应急事件风险防范措施的评估。评估的主要内容是分析控制措施的有效性、应急预案的完备性、应急演练的全面性和及时性，改进风险控制措施，完善应急预案，促进风险防范措施的持续改进。