YD

中华人民共和国通信行业标准

YD/T 1731-2008

电信网和互联网灾难备份及恢复实施指南

Implementation Guide for Disaster Backup and Recovery of Telecom Network and Internet

2008-01-14 发布　　2008-01-14 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称如下：

1. YD/T 1728-2008　电信网和互联网安全防护管理指南；
2. YD/T 1729-2008　电信网和互联网安全等级保护实施指南；
3. YD/T 1730-2008　电信网和互联网安全风险评估实施指南；
4. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南；
5. YD/T 1732-2008　固定通信网安全防护要求；
6. YD/T 1733-2008　固定通信网安全防护检测要求；
7. YD/T 1734-2008　移动通信网安全防护要求；
8. YD/T 1735-2008　移动通信网安全防护检测要求；
9. YD/T 1736-2008　互联网安全防护要求；
10. YD/T 1737-2008　互联网安全防护检测要求；
11. YD/T 1738-2008　增值业务网——消息网安全防护要求；
12. YD/T 1739-2008　增值业务网——消息网安全防护检测要求；
13. YD/T 1740-2008　增值业务网——智能网安全防护要求；
14. YD/T 1741-2008　增值业务网——智能网安全防护检测要求；
15. YD/T 1742-2008　接入网安全防护要求；
16. YD/T 1743-2008　接入网安全防护检测要求；
17. YD/T 1744-2008　传送网安全防护要求；
18. YD/T 1745-2008　传送网安全防护检测要求；
19. YD/T 1746-2008　IP承载网安全防护要求；
20. YD/T 1747-2008　IP承载网安全防护检测要求；
21. YD/T 1748-2008　信令网安全防护要求；
22. YD/T 1749-2008　信令网安全防护检测要求；
23. YD/T 1750-2008　同步网安全防护要求；
24. YD/T 1751-2008　同步网安全防护检测要求；
25. YD/T 1752-2008　支撑网安全防护要求；
26. YD/T 1753-2008　支撑网安全防护检测要求；
27. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求；
28. YD/T 1755-2008　电信网和互联网物理环境安全等级保护检测要求；
29. YD/T 1756-2008　电信网和互联网管理安全等级保护要求；
30. YD/T 1757-2008　电信网和互联网管理安全等级保护检测要求；
31. YD/T 1758-2008　非核心生产单元安全防护要求；
32. YD/T 1759-2008　非核心生产单元安全防护检测要求。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准的附录A是资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、中国移动通信集团公司、中国电信集团公司、中国网络通信集团公司、中国铁通集团有限公司

本标准主要起草人：杨　洋、田慧蓉、陈　欣、王新峰、殷　琪、刘立松

电信网和互联网灾难备份及恢复实施指南

1 范围

本标准对电信网和互联网灾难备份及恢复工作的目标和原则进行了描述和规范。同时，规定了电信网和互联网灾难备份及恢复工作的基本实施方法。

本标准适用于电信网和互联网的灾难备份及恢复工作。

本标准可作为电信网和互联网灾难备份及恢复的总体指导性文件，针对具体网络的灾难备份及恢复可参考具体网络的安全防护要求和安全防护检测要求。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

3 术语和定义

GB/T 5271.8-2001确立的术语和定义以及下列术语和定义适用于本标准。

3.1

电信网 Telecom Network

利用有线和/或无线的电磁、光电系统，进行文字、声音、数据、图像或其他任何媒体的信息传递的网络，包括固定通信网、移动通信网等。

3.2

互联网 Internet

泛指广域网、局域网及终端（包括计算机、手机等）通过交换机、路由器、网络接入设备等基于一定的通信协议连接形成的，功能和逻辑上的大型网络。

3.3

电信网和互联网灾难 Disaster of Telecom Network and Internet

由于各种原因，造成电信网和互联网及相关系统故障或瘫痪，使电信网和互联网及相关系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.4

电信网和互联网灾难备份 Backup for Disaster Recovery of Telecom Network and Internet

为了电信网和互联网及相关系统灾难恢复而对相关网络要素进行备份的过程。

3.5

电信网和互联网灾难恢复 Disaster Recovery of Telecom Network and Internet

为了将电信网和互联网及相关系统从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.6

电信网和互联网安全防护体系 Security Protection Architecture of Telecom Network and Internet

电信网和互联网的安全等级保护、安全风险评估、灾难备份及恢复三项工作互为依托、互为补充、相互配合，共同构成了电信网和互联网安全防护体系。

3.7

电信网和互联网安全等级 Security Classification of Telecom Network and Internet

电信网和互联网及相关系统重要程度的表征。重要程度从电信网和互联网及相关系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.8

电信网和互联网安全等级保护 Classified Security Protection of Telecom Network and Internet

指对电信网和互联网及相关系统分等级实施安全保护。

3.9

电信网和互联网安全风险 Security Risk of Telecom Network and Internet

人为或自然的威胁可能利用电信网和互联网及相关系统存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.10

电信网和互联网安全风险评估 Security Risk Assessment of Telecom Network and Internet

指运用科学的方法和手段，系统地分析电信网和互联网及相关系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全措施，防范和化解电信网和互联网及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障电信网和互联网及相关系统的安全提供科学依据。

3.11

业务影响分析 Business Impact Analysis

分析业务功能及其相关电信网和互联网资源、评估特定灾难对各种业务功能的影响的过程。

3.12

电信网和互联网灾难恢复预案 Disaster Recovery Plan of Telecom Network and Internet

定义电信网和互联网灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复电信网和互联网的数据、作业能力和业务功能。

3.13

演练 Exercise

为训练人员和提高电信网和互联网灾难恢复能力而根据电信网和互联网灾难恢复预案进行活动的过程。

3.14

电信网和互联网相关系统 System of Telecom Network and Internet

组成电信网和互联网的相关系统，包括接入网、传送网、IP承载网、信令网、同步网、支撑网等。其中，接入网包括各种有线、无线和卫星接入网等，传送网包括光缆、波分、SDH、卫星等，而支撑网则包括业务支撑和网管系统。

4 电信网和互联网灾难备份及恢复概述

4.1 灾难备份及恢复的工作目标

电信网和互联网灾难备份及恢复的工作目标是：在电信网和互联网安全防护体系的框架下，依据电信网和互联网安全等级保护的定级结果和安全风险评估的相关信息，结合网络和业务运营商自身的实际情况，分析电信网和互联网及相关系统不同等级的安全需求，平衡效益与成本，制定灾难备份及恢复策略，在此基础上实现灾难备份技术方案，构建并执行灾难恢复预案，以便于提高电信网和互联网抵御灾难的能力，尽可能减小因灾难引起的各种损失，从而增强电信网和互联网的安全防护能力和持续作业能力，使电信网和互联网能够完成其使命。

4.2 灾难备份及恢复的工作原则

电信网和互联网灾难备份及恢复工作应首先满足电信网和互联网安全防护工作提出的适度安全原则、标准性原则、可控性原则、完备性原则、最小影响原则以及保密性原则。在此基础上，电信网和互联网灾难备份及恢复工作在实施过程中还应重点遵循以下原则。

——统筹规划原则：灾难备份及恢复要统筹考虑，合理布局，避免重复建设。

——资源共享原则：灾难备份及恢复要充分利用现有资源，讲究实效，保证重点。

——“平战结合”原则：应将日常运营与灾难备份及恢复需求结合起来，综合安排。

——可靠性原则：灾难备份及恢复要确保备份技术和设施的可靠性以及恢复能力的可靠性。

——一致性原则：灾难备份及恢复应与电信网和互联网安全防护体系的相关要求保持一致，依据安全等级保护的评定结果确定灾难备份及恢复等级，充分考虑安全风险评估的相关结论。

4.3 灾难备份及恢复的管理

网络和业务运营商应对电信网和互联网灾难备份及恢复工作进行需求分析，落实资源管理，以便于筹备调配所需资源、制定合理的工作策略、协调各结构和不同人员之间的活动和工作。在此基础上应确定详细任务及时间表，从而有效保证灾难备份及恢复策略的规范实施。在实施过程中应始终跟踪和报告任务进展并进行问题管理和变更管理。

4.4 灾难备份及恢复的备案和审计

电信网和互联网灾难备份及恢复的等级划分、需求分析、策略制定、灾难备份技术方案的设计实现、灾难恢复预案的制定等相关活动，应按有关规定进行备案和审计。

5 电信网和互联网灾难备份及恢复等级划分

5.1 灾难备份及恢复定级原则

根据电信网和互联网安全防护体系的相关要求，安全等级保护工作为灾难备份及恢复的实施提供等级划分指导，灾难备份及恢复的等级应与安全等级保护确定的安全等级一致，因此电信网和互联网灾难备份及恢复分为以下5个等级。

——第 1 级：定级对象受到破坏后，会对网络和业务运营商的合法权益造成轻微损害，但不损害国家安全、社会秩序、经济运行和公共利益。

本级由定级对象的所有者依据国家和通信行业有关标准进行保护。

——第 2 级：定级对象受到破坏后，会对网络和业务运营商的合法权益产生严重损害，或者对社会秩序、经济运行和公共利益造成轻微损害，但不损害国家安全。

本级由定级对象的所有者依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行指导。

——第 3 级：进一步划分为两个级别：

● 第 3.1 级：定级对象受到破坏后，会对网络和业务运营商的合法权益产生特别严重损害，或者对社会秩序、经济运行和公共利益造成较大损害，或者对国家安全造成轻微损害。

本级由定级对象的所有者依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行监督、检查。

● 第 3.2 级：定级对象受到破坏后，会对网络和业务运营商的合法权益产生特别严重损害，或者对社会秩序、经济运行和公共利益造成严重损害，或者对国家安全造成较大损害。

本级由定级对象的所有者依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行重点监督、检查。

——第 4 级：定级对象受到破坏后，会对社会秩序、经济运行和公共利益造成特别严重损害，或者对国家安全造成严重损害。

本级由定级对象的所有者依据国家和通信行业有关标准以及业务的特殊安全要求进行保护，主管部门对其安全等级保护工作进行强制监督、检查。

——第 5 级：定级对象受到破坏后，会对国家安全造成特别严重损害。

本级由定级对象的所有者依据国家和通信行业有关标准以及业务的特殊安全需求进行保护，主管部门对其安全等级保护工作进行专门监督、检查。

根据上述定级原则，结合电信网和互联网的特点，选取和定义支持灾难备份及恢复实施工作的资源要素。在此基础上可对各实施资源要素分别提出不同等级的要求，实现对电信网和互联网灾难备份及恢复的等级划分。电信网和互联网要达到某个灾难备份及恢复等级，应同时满足该等级中所有实施资源要素的要求。针对具体的电信网和互联网及相关系统，其灾难备份及恢复的实施资源要素以及这些实施资源要素针对不同灾难备份及恢复等级的要求应参见具体网络的安全防护要求和安全防护检测要求。

5.2 灾难备份及恢复实施资源要素

可将支持电信网和互联网灾难备份及恢复各个等级所需的资源分为以下6个要素：

——冗余系统、冗余设备及冗余链路：指在电信网和互联网组网、优化阶段部署的各种冗余系统、冗余设备以及冗余通信链路等；

——冗余路由：指电信网和互联网在路由层面的冗余性设计；

——备份数据：指电信网和互联网各种数据的备份；

——人员和技术支持能力：对电信网和互联网灾难备份及恢复的实施安排相关人员、提供支撑和综合保障的能力，以实现灾难备份及恢复的预期目标。包括对电信网和互联网及其信息系统安全运行的管理能力、问题分析处理能力等；

——运行维护管理能力：包括电信网和互联网运行环境管理、数据管理、资源管理、信息系统管理、安全管理和变更管理等；

——灾难恢复预案：用于指导电信网和互联网灾难恢复工作的执行方案，包括各种资源的调配、人员处置以及系统、业务、数据的恢复流程等。

5.3 灾难备份及恢复实施等级要求

根据电信网和互联网灾难备份及恢复定级原则、支持灾难备份及恢复实施的6个资源要素，可对每个等级的实施进行具体要求如下。

5.3.1 第1级

不作要求。

5.3.2 第2级

第2级灾难备份及恢复应具有的技术和管理支持如表1所示。

表1 第2级

实施资源要素	要 求
冗余系统、冗余设备及冗余链路	a） 可从系统、设备、链路的设计部署等方面实施； b） 单节点的灾难不应导致其他节点的作业能力和业务提供发生异常；单一地区范围的灾难不应导致其他地区的作业能力和业务提供发生异常； c） 网络灾难恢复时间应满足相关要求
冗余路由	a） 有路由的冗余设计； b） 网络收敛时间应满足相关要求
备份数据	a） 有重要数据备份； b） 数据备份范围和时间间隔、数据恢复能力应满足相关要求
人员和技术支持能力	a） 有负责机房运行的管理人员。
运行维护管理能力	a） 有机房运行管理制度； b） 有介质存取、验证和转储管理制度，确保备份数据授权访问
灾难恢复预案	a） 有灾难恢复预案

5.3.3 第3.1级

3.1级灾难备份及恢复应具有的技术和管理支持如表2所示。

表2 3.1级

实施资源要素	要 求
冗余系统、冗余设备及冗余链路	a） 可从系统、设备、链路的设计部署等方面实施； b） 单节点的灾难不应导致其他节点的作业能力和业务提供发生异常；单一地区范围的灾难不应导致其他地区的作业能力和业务提供发生异常； c） 网络灾难恢复时间应满足相关要求
冗余路由	a） 有路由的冗余设计； b） 网络收敛时间应满足相关要求
备份数据	a） 有重要数据备份； b） 数据备份范围和时间间隔、数据恢复能力应满足相关要求
人员和技术支持能力	a） 有负责机房运行管理的人员； b） 有负责灾难备份及恢复工作的技术支持人员； c） 对技术支持人员有定期的技术培训
运行维护管理能力	a） 有机房运行管理制度； b） 有介质存取、验证和转储管理制度，确保备份数据授权访问； c） 按介质特性对备份数据进行定期的有效性验证； d） 有硬件、网络运行管理制度； e） 有数据容灾备份管理制度； f） 与外部组织保持良好的联络和协作能力
灾难恢复预案	a） 有完整的灾难恢复预案； b） 有灾难恢复预案的教育和培训； c） 有灾难恢复预案的的演练

5.3.4 第3.2级

3.2级灾难备份及恢复应具有的技术和管理支持如表3所示。

表3 3.2级

实施资源要素	要 求
冗余系统、冗余设备及冗余链路	a） 可从系统、设备、链路的设计部署等方面实施； b） 单节点的灾难不应导致其他节点的作业能力和业务提供发生异常；单一地区范围的灾难不应导致其他地区的作业能力和业务提供发生异常； c） 网络灾难恢复时间应满足相关要求
冗余路由	a） 有路由的冗余设计； b） 有流量负荷分担设计； c） 网络收敛时间应满足相关要求
备份数据	a） 有重要数据备份； b） 数据备份范围和时间间隔、数据恢复能力应满足相关要求
人员和技术支持能力	a） 有负责机房运行管理的人员； b） 有负责灾难备份及恢复工作的技术支持人员； c） 对技术支持人员有定期的技术培训
运行维护管理能力	a） 有机房运行管理制度； b） 有介质存取、验证和转储管理制度，确保备份数据授权访问； c） 按介质特性对备份数据进行定期的有效性验证； d） 有硬件、网络运行管理制度； e） 有操作系统、数据库、应用软件运行管理制度； f） 有数据容灾备份管理制度； g） 与外部组织保持良好的联络和协作能力
灾难恢复预案	a） 有完整的灾难恢复预案； b） 有灾难恢复预案的教育和培训； c） 有灾难恢复预案的的演练； d） 有完善的灾难恢复预案管理制度

5.3.5 第4级

待补充。

5.3.6 第5级

待补充。

6 电信网和互联网灾难备份及恢复需求分析

根据电信网和互联网安全等级保护所确定的安全等级，确定电信网和互联网灾难备份及恢复的等级和目标，包括以下两点：

——电信网和互联网及相关系统的灾难备份及恢复等级：与安全等级保护所确定的安全等级一致；

——电信网和互联网及相关系统、业务的灾难恢复指标范围，包括网络或业务恢复顺序、灾难备份及恢复的实施资源要素等。

7 电信网和互联网灾难备份及恢复策略的制定

7.1 灾难备份及恢复策略的制定方法

按照灾难备份及恢复实施资源要素的成本应与灾难可能造成的损失之间取得平衡的原则（以下简称“成本风险平衡原则”），根据电信网和互联网灾难备份及恢复的等级和目标，确定电信网和互联网及相关系统的灾难备份及恢复策略，不同的电信网和互联网及相关系统可采用不同的灾难备份及恢复策略。

制定电信网和互联网灾难备份及恢复策略需要明确：

——灾难备份及恢复实施资源要素的获取方式；

——灾难备份及恢复实施资源要素的具体要求。

7.2 灾难备份及恢复实施资源要素的获取方式

7.2.1 冗余系统、冗余设备及冗余链路

系统、设备和链路部署的冗余性由网络和业务运营商在组网、优化阶段进行获取。

7.2.2 冗余路由

为获取路由的冗余性，需设备制造商在设备设计、生产阶段实现相关功能，并由网络和业务运营商在组网、优化阶段进行设计部署。

7.2.3 备份数据

数据由网络和业务运营商自行维护并备份。

7.2.4 人员和技术支持能力

可选用以下两种方式来设置人员并获取技术支持能力：

——由网络和业务运营商自行设置技术支持人员；

——由网络和业务运营商与设备制造商或其他厂商签订技术支持或服务合同。

7.2.5 运行维护管理能力

可选用以下两种方式来获取运行维护管理能力：

——由网络和业务运营商自行运行、维护和管理；

——由网络和业务运营商委托其他机构运行、维护和管理。

7.2.6 灾难恢复预案

可选用以下三种方式完成灾难恢复预案的制定、落实和管理：

——由网络和业务运营商独立完成；

——由网络和业务运营商聘请外部专家指导完成；

——由网络和业务运营商委托外部机构完成。

7.3 灾难备份及恢复实施资源要素的具体要求

7.3.1 冗余系统、冗余设备及冗余链路

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下几项内容：

——系统、设备及链路部署的冗余性；

——系统的处理能力、设备及链路的容量等相关参数；

——网络链路保护倒换的速度；

——机房其他设备的冗余性。

7.3.2 冗余路由

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下三项内容：

——网络路由设计的冗余性；

——网络是否支持流量负荷分担；

——网络收敛速度。

7.3.3 备份数据

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下几项内容：

——系统关键数据的组成；

——数据备份的形式；

——数据备份的范围；

——数据备份的时间间隔；

——数据备份系统的组成设备；

——数据备份的技术；

——数据备份介质的可靠性及容量。

7.3.4 人员和技术支持能力

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下三项内容：

——技术支持的组织架构；

——在硬件、软件、网络、工作时间等方面的技术支持要求；

——各类技术支持人员的数量和素质等要求。

7.3.5 运行维护管理能力

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下几项内容：

——运行维护管理的组织架构；

——各类运行维护管理人员的数量和素质等要求；

——数据备份及访问授权的管理制度；

——机房、硬件、网络、软件的运行管理制度；

——与外部组织的联络和协作能力。

7.3.6 灾难恢复预案

网络和业务运营商应根据灾难备份及恢复等级和目标，按照成本风险平衡原则，确定以下几项内容：

——灾难恢复预案的整体要求；

——灾难恢复预案的制定和实现要求；

——灾难恢复预案的教育、培训和演练要求；

——灾难恢复预案的管理要求。

8 电信网和互联网灾难备份及恢复策略的实现

8.1 灾难备份及恢复策略的实现方法

参照所确定的灾难备份及恢复实施资源要素的获取方式和具体要求，可从6个不同的实施资源要素入手，实现所制定的灾难备份及恢复策略。

电信网和互联网灾难备份及恢复策略的实现包括以下关键部分：

——灾难备份技术方案的实现；

——人员和技术支持能力的实现；

——运行维护管理能力的实现；

——灾难恢复预案的实现。

8.2 灾难备份技术方案的实现

8.2.1 技术方案的设计、验证和确认

网络和业务运营商应根据灾难备份及恢复策略制定相应的灾难备份技术方案，需考虑冗余系统、冗余设备及冗余链路、冗余路由和备份数据等要素。

——技术方案应遵循成本风险平衡原则；

——技术方案应具有可扩展性；

——技术方案应具有高可靠性。

网络和业务运营商在选择数据异地容灾备份地点时，应遵循以下原则：

——与本地之间的地理距离和相应风险匹配；

——避免与本地同时遭受同类风险；

——与本地之间通信的设施安全可靠。

为确保技术方案满足电信网和互联网灾难备份及恢复策略的要求，应由网络和业务运营商的相关部门对技术方案进行验证和确认，并记录、保存验证和确认的结果。

8.2.2 技术方案的部署和测试

网络和业务运营商应按照确认的灾难备份技术方案进行相应部署，增加系统、链路和路由的冗余性，并按要求对数据进行备份。

网络和业务运营商应按照确认的灾难备份技术方案和部署情况制定相应测试计划，并组织用户共同进行测试。测试内容主要包括：

——网络部署规划对系统和设备冗余性的支持；

——网络链路的保护倒换功能及速度；

——网络重路由功能及网络收敛速度；

——网络流量负荷分担功能；

——本地备份数据的恢复功能；

——数据的异地备份功能；

——异地备份数据的恢复功能。

8.3 人员和技术支持能力的实现

根据所制定的灾难备份及恢复策略，网络和业务运营商应做到以下三点：

——获取硬件、软件、网络、工作时间等方面的相应技术支持能力；

——建立相应的技术支持组织；

——定期对技术支持人员进行操作技能培训。

8.4 运行维护管理能力的实现

为了达到灾难备份及恢复目标，网络和业务运营商按照所制定的灾难备份及恢复策略应做到以下几点：

——建立各种完善的操作和管理制度；

——确保数据备份的安全性、及时性、有效性和可靠性；

——与外部组织保持良好的联络和协作能力；

——确保有效的应急响应和处理能力；

——定期对相关人员进行安全管理教育培训。

8.5 灾难恢复预案的实现

8.5.1 灾难恢复预案的制定

电信网和互联网灾难恢复预案的制定应遵循以下原则：

——完整性：灾难恢复预案应包含灾难恢复的整个过程，以及灾难恢复所需的尽可能全面的数据和资料；

——易用性：灾难恢复预案应使用易于理解的语言和图表，并适合在紧急情况下使用；

——明确性：灾难恢复预案应采用清晰的结构，对电信网和互联网资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人；

——有效性：灾难恢复预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际电信网、互联网和人员组织的同步更新；

——兼容性：灾难恢复预案应与国家和行业其他应急预案体系有机结合。

电信网和互联网灾难恢复预案制定的过程如下：

——起草：参照附录 A 灾难恢复预案框架，按照风险分析、相关系统和业务影响分析所确定的灾难备份及恢复内容，根据灾难备份及恢复等级的要求，参考国家和行业其他相关的应急预案，撰写灾难恢复预案的初稿。

——评审：应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相应的流程保证。

——测试：应预先制定测试计划，在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录，并形成测试报告。

——修订：根据评审和测试结果，对灾难恢复预案进行修订，纠正在初稿评审过程和测试中发现的问题和缺陷，形成灾难恢复预案的报批稿。

——审核和批准：由网络和业务运营商的决策层对报批稿进行审核和批准，确定为灾难恢复预案的执行稿。

8.5.2 灾难恢复预案的教育、培训和演练

为了使相关人员了解电信网和互联网灾难恢复的目标和流程，熟悉灾难恢复的操作规程，网络和业务运营商应按以下要求，组织灾难恢复预案的教育、培训和演练。

——在电信网和互联网运行的整个生命周期都应进行灾难恢复观念的宣传教育工作。

——应预先对培训需求进行评估，开发和落实相应的培训及教育课程，保证课程内容与灾难恢复预案的要求相一致。

——应事先确定培训的频次和范围，事后保留培训的记录。

——预先制定演练计划，在计划中说明演练的场景。

——演练的整个过程应有详细的记录，并形成报告；

——应定期组织有最终用户参与的完全演练。

8.5.3 灾难恢复预案的管理

经过审核和批准的灾难恢复预案，应具备以下几点：

——由专人负责保存与分发；

——具有多份拷贝在不同的地点保存；

——分发给参与灾难恢复工作的所有人员；

——在每次修订后所有拷贝统一更新，并保留以备查阅，原分发的旧版本应予销毁。

为了保证灾难恢复预案的有效性，应从以下方面对灾难恢复预案进行严格的维护和变更管理：

——电信网和互联网及相关系统结构的变化、业务的变更、人员的变更都应在灾难恢复预案中及时反映；

——灾难恢复预案在测试、演练和灾难发生后实际执行时，其过程均应有详细的记录，并应对测试、演练和执行的效果进行评估，同时对灾难恢复预案进行相应的修订；

——灾难恢复预案应根据电信网和互联网实际情况定期评审和修订。

附 录 A
（资料性附录）
电信网和互联网灾难恢复预案框架

A.1 恢复目标和范围

定义电信网和互联网灾难恢复预案中的相关术语和方法论，并说明电信网和互联网灾难恢复的目标，如恢复时间目标等。说明灾难恢复预案的作用范围，解决哪些问题，不解决哪些问题。

A.2 组织机构和职责

描述电信网和互联网灾难恢复组织机构的组成、各个岗位的职责和人员名单。灾难恢复组织机构应包括应急响应组和灾难恢复组等。

A.3 联络和通信

列出电信网和互联网灾难恢复相关人员和组织机构的联络表，包含主管部门、灾难恢复团队、设备制造商、安全服务商、其他厂商、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。

A.4 应急响应流程

A.4.1 事件通告

任何人员在发现电信网和互联网紧急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。

A.4.2 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。

A.4.3 损害评估

在电信网和互联网紧急事件发生后，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紧急事件进行慎重评估，确认紧急事件对电信网和互联网造成的影响程度，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。

A.4.4 灾难宣告

应预先制定电信网和互联网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，网络和业务运营商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。

A.5 恢复流程

利用备份技术方案、人员和技术支持能力、运行维护管理能力恢复电信网和互联网及相关系统的作业能力以及业务功能的提供。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。

A.6 预案的保障条件

——专业技术保障；
——通信保障；
——电力保障；
——后勤保障。

A.7 预案附录

——人员疏散计划；
——设备说明书；
——服务级别协议和备忘录；
——资源清单；
——电信网和互联网及相关系统、业务影响分析报告；
——预案的保存和分发办法。

参 考 文 献

1. YD/T 1729-2008 电信网和互联网安全等级保护实施指南
2. YD/T 1730-2008 电信网和互联网风险评估实施指南
3. GB/T 20988-2007 信息系统灾难恢复规范