YD

中华人民共和国通信行业标准

YD/T 1752-2008

支撑网安全防护要求

Security Protection Requirements for Supporting Network

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。

本标准与YD/T 1753-2008《支撑网安全防护检测要求》配套使用。

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、中国铁通集团有限公司、中国电信集团公司、中国移动通信集团公司、中国网络通信集团公司、中国联合通信有限公司

本标准主要起草人：李　成、胡　新、唐建军、田　峰、刘险峰、王君珂、徐　楠

支撑网安全防护要求

1 范围

本标准规定了支撑网在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公众电信网中的支撑网。

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本标准的条款。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。

YD/T 1729-2008　电信网和互联网安全等级保护实施指南

YD/T 1730-2008　电信网和互联网安全风险评估实施指南

YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南

YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求

YD/T 1756-2008　电信网和互联网管理安全等级保护要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

支撑网安全等级 Security Classification of Supporting Network

支撑网安全重要程度的表征。重要程度可从支撑网受到破坏后，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。

3.2

支撑网安全等级保护 Classified Security Protection of Supporting Network

对支撑网分等级实施安全保护。

3.3

组织 Organization

组织是由不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.4

支撑网安全风险 Security Risk of Supporting Network

人为或自然的威胁可能利用支撑网中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。

3.5

支撑网安全风险评估 Security Risk Assessment of Supporting Network

指运用科学的方法和手段，系统地分析支撑网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。防范和化解支撑网安全风险，或者将风险控制在可接受的水平，为最大限度地为保障支撑网的安全提供科学依据。

3.6

支撑网资产 Asset of Supporting Network

支撑网中具有价值的资源，是安全防护保护的对象。支撑网中的资产可能以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如网络管理系统、计费系统等。

3.7

支撑网资产价值 Asset Value of Supporting Network

支撑网中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.8

支撑网威胁 Threat of Supporting Network

可能导致对支撑网产生危害的不希望事故的潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的支撑网威胁有黑客入侵、硬件故障、人为操作失误、火灾、水灾等等。

3.9

支撑网脆弱性 Vulnerability of Supporting Network

支撑网脆弱性是指支撑网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危害资产的安全。

3.10

支撑网灾难 Disaster of Supporting Network

由于各种原因，造成支撑网故障或瘫痪，使支撑网的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。

3.11

支撑网灾难备份 Backup for Disaster Recovery of Supporting Network

为了支撑网灾难恢复而对相关网络要素进行备份的过程。

3.12

支撑网灾难恢复 Disaster Recovery of Supporting Network

为了将支撑网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。

4 支撑网安全防护概述

4.1 支撑网安全防护范围

支撑网是独立于业务网之外的用于支持网络及设备维护、业务运营和账务管理的综合信息系统所组成的网络。本标准中支撑网的安全防护范围包括网管系统和业务运营支撑系统。本标准中的网管系统覆盖以下网络：固定通信网、移动通信网、消息网、智能网、接入网、传送网、IP承载网、信令网、同步网。本标准中的业务运营支撑系统包括计费系统、营业系统、账务系统。

4.2 支撑网安全防护内容

根据电信网和互联网安全防护体系的要求，将支撑网安全防护内容分为安全等级保护、安全风险评估、灾难备份及恢复等3个部分。

——支撑网安全等级保护

主要包括业务安全、网络安全、主机安全、应用安全、数据安全及备份恢复、物理环境安全、管理安全等。

——支撑网安全风险评估

主要包括资产识别、脆弱性识别、威胁识别、已有安全措施的确认、风险分析、风险评估文件记录等，本标准文件仅对支撑网进行资产分析、脆弱性分析、威胁分析，在支撑网安全风险评估过程中确定各个资产、脆弱性、威胁的具体值。资产、脆弱性、威胁的赋值方法及资产价值、风险值的计算方法参见YD/T 1730-2008《电信网和互联网安全风险评估实施指南》。

——支撑网灾难备份及恢复

主要包括灾难备份及恢复等级确定、针对灾难备份及恢复各资源要素的具体实施等。

5 支撑网定级对象和安全等级确定

本标准文件中支撑网的定级对象为各类网管系统和业务运营支撑系统，可按照全国、省和地市将各个系统分为不同级别。网络和业务运营商应根据YD/T 1729-2008《电信网和互联网安全等级保护实施指南》中确定安全等级的方法对支撑网进行定级，即根据社会影响力、所提供服务的重要性、规模和服务范围的大小对各类网管系统和业务运营支撑系统分别定级。定级方法中的权重α、β、γ可根据具体网络情况进行调节。

6 支撑网资产、脆弱性、威胁分析

6.1 资产分析

支撑网的资产可分为设备硬件、软件、数据、网络、服务、文档和人员等。表1给出支撑网的资产列表。

表1 支撑网资产列表

分 类	示 例
设备硬件	支撑网中的各种主机设备，网络设备
设备软件	设备中的软件，包括操作系统、中间件软件、数据库软件、应用软件等
重要数据	保存在设备上的各种重要数据，包括网元和网络配置数据、管理员操作维护记录、用户信息、计费数据和账单等
网络	承载支撑网的网络
服务	账单服务等
文档	纸质以及保存在电脑中的各种文件，如设计文档、技术要求、管理规定（机构设置、管理制度、人员管理办法）、工作计划、技术或财务报告、用户手册等
人员	管理人员，掌握重要技术的人员，如网络维护人员、设备维护人员、研发人员等

6.2 脆弱性分析

支撑网的脆弱性可分为技术脆弱性和管理脆弱性两方面。表2给出支撑网的脆弱性列表。

表2 支撑网脆弱性列表

类 型	对 象	存在的脆弱性
技术脆弱性	服务/应用	由于网络和设备的处理或备份能力不够而导致服务提供不连续
	网络	网络拓扑设计不合理，无冗余链路，单点故障隐患，与互联网连接造成的访问控制漏洞
	设备（软件、硬件和数据）	设备老化、系统设计缺陷、无数据备份、无过载保护、无防病毒黑客攻击的手段等系统存在可被外界利用的漏洞
	物理环境	机房场地选择不合理，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范；通信线路、机房设备的保护不符合规范
管理脆弱性		（1）安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； （2）安全管理制度方面：管理制度不完善、制度评审和修订不及时等； （3）人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于外部人员未进行限制访问等； （4）建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； （5）运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位等

6.3 威胁分析

支撑网的威胁可分为设备威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表3给出支撑网的威胁列表。

表3 支撑网威胁列表

来 源		威胁描述
设备威胁		各类设备本身的软硬件故障，设备和介质老化造成的数据丢失，系统宕机
环境威胁	物理环境	断电、静电、灰尘、潮湿、温度、电磁干扰等；意外事故或通信线路方面的故障
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷电
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏； 采用自主或内外勾结的方式盗窃或篡改机密信息； 外部人员利用恶意代码和病毒对网络或系统进行攻击； 外部人员进行物理破坏、盗窃等
	非恶意人员	内部人员由于缺乏责任心或者无作为而没有执行应当执行的操作，或无意地执行了错误的操作导致安全事件； 内部人员没有遵循规章制度和操作流程而导致故障或信息损坏； 内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击； 安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件

7 支撑网安全等级保护要求

7.1 第1级要求

不作要求。

7.2 第2级要求

7.2.1 业务安全

a）计费系统要求不间断运行，全年中断时间应符合电信运营企业的相关要求；

b）计费系统中断后应当对中断期间未采集的数据进行补采；

c）计费系统定时对计费信息等数据进行备份，保证计费信息不丢失，计费数据在系统中保存的时间应符合相关要求（至少3个月）；

d）账务系统应当确保账单的准确性，保证账单不重复、不丢失、不被修改。

7.2.2 网络安全

7.2.2.1 结构安全

a）应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

b）应保证接入网络和核心网络的带宽满足业务高峰期需要；

c）应绘制与当前运行情况相符的网络拓扑结构图；

d）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

7.2.2.2 访问控制

a）应在网络边界部署访问控制设备，启用访问控制功能；

b）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级；

c）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

7.2.2.3 安全审计

a）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

7.2.2.4 边界完整性检查

应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

7.2.2.5 入侵防范

应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

7.2.2.6 网络设备防护

a）应对登录网络设备的用户进行身份鉴别；

b）应对网络设备的管理员登录地址进行限制；

c）网络设备用户的标识应惟一；

d）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

e）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

f）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.2.3 主机安全

7.2.3.1 身份鉴别

a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有惟一性。

7.2.3.2 访问控制

a）应启用访问控制功能，依据安全策略控制用户对资源的访问；

b）应实现操作系统和数据库系统特权用户的权限分离；

c）应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；

d）应及时删除多余的、过期的账户，避免共享账户的存在。

7.2.3.3 安全审计

a）审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；

b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d）应保护审计记录，避免受到未预期的删除、修改或覆盖等。

7.2.3.4 入侵防范

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

7.2.3.5 恶意代码防范

a）应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b）应支持防恶意代码软件的统一管理。

7.2.3.6 资源控制

a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b）应根据安全策略设置登录终端的操作超时锁定；

c）应限制单个用户对系统资源的最大或最小使用限度。

7.2.4 应用安全

7.2.4.1 身份鉴别

a）应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b）应提供用户身份标识惟一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

c）应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d）应启用身份鉴别、用户身份标识惟一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

7.2.4.2 访问控制

a）应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b）访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

c）应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；

d）应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

7.2.4.3 安全审计

a）应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

b）应保证无法删除、修改或覆盖审计记录；

c）审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

7.2.4.4 通信完整性

应采用校验码技术保证通信过程中数据的完整性。

7.2.4.5 通信保密性

a）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

b）应对通信过程中的敏感信息字段进行加密。

7.2.4.6 软件容错

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

7.2.4.7 资源控制

a）当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b）应能够对应用系统的最大并发会话连接数进行限制；

c）应能够对单个账户的多重并发会话进行限制。

7.2.5 数据安全及备份恢复

7.2.5.1 数据完整性

应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

7.2.5.2 数据保密性

应采用加密或其他保护措施实现鉴别信息的存储保密性。

7.2.5.3 备份和恢复

a）应能够对重要信息进行备份和恢复；

b）应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

7.2.6 物理环境安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中的第2级要求。

7.2.7 管理安全

应满足 YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中的第 2 级要求。

7.3 第 3.1 级要求

7.3.1 业务安全

与7.2.1的要求相同。

7.3.2 网络安全

7.3.2.1 结构安全

除满足7.2.2.1的要求之外，还应满足：

a）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

b）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

c）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

7.3.2.2 访问控制

除满足7.2.2.2的要求之外，还应满足：

a）应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；

b）应在会话处于非活跃一定时间或会话结束后终止网络连接；

c）应限制网络最大流量数及网络连接数；

d）重要网段应采取技术手段防止地址欺骗。

7.3.2.3 安全审计

除满足7.2.2.3的要求之外，还应满足：

a）应能够根据记录数据进行分析，并生成审计报表；

b）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

7.3.2.4 边界完整性检查

除满足7.2.2.4的要求之外，还应满足：

应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

7.3.2.5 入侵防范

除满足7.2.2.5的要求之外，还应满足：

当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

7.3.2.6 网络设备防护

除满足7.2.2.6的要求之外，还应满足：

应实现设备特权用户的权限分离。

7.3.2.7 恶意代码防范

a）应在网络边界处对恶意代码进行检测和清除；

b）应维护恶意代码库的升级和检测系统的更新。

7.3.3 主机安全

7.3.3.1 身份鉴别

与7.2.3.1的要求相同。

7.3.3.2 访问控制

除满足7.2.3.2的要求之外，还应满足：

a）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

b）应对重要信息资源设置敏感标记；

c）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

7.3.3.3 安全审计

除满足7.2.3.3的要求之外，还应满足：

a）应能够根据记录数据进行分析，并生成审计报表；

b）应保护审计进程，避免受到未预期的中断。

7.3.3.4 入侵防范

除满足7.2.3.4的要求之外，还应满足：

a）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

b）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

7.3.3.5 恶意代码防范

除满足7.2.3.5的要求之外，还应满足：

主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

7.3.3.6 资源控制

除满足7.2.3.6的要求之外，还应满足：

a）应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

b）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

7.3.4 应用安全

7.3.4.1 身份鉴别

与7.2.4.1的要求相同。

7.3.4.2 访问控制

除满足7.2.4.2的要求之外，还应满足：

a）应具有对重要信息资源设置敏感标记的功能；

b）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

7.3.4.3 安全审计

除满足7.2.4.3的要求之外，还应满足:

a）应保证无法单独中断审计进程；

b）应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

c）对涉及金额的数据以及涉及用户信息数据的访问，应强化审计，有能力发现内部滥用行为。

7.3.4.4 通信完整性

除满足7.2.4.4的要求之外，还应满足:

应采用密码技术保证通信过程中数据的完整性。

7.3.4.5 通信保密性

与7.2.4.5的要求相同。

7.3.4.6 软件容错

除满足7.2.4.6的要求之外，还应满足:

应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

7.3.4.7 资源控制

除满足7.2.4.7的要求之外，还应满足：

a）应能够对一个时间段内可能的并发会话连接数进行限制；

b）应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

c）应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

d）应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

7.3.5 数据安全及备份恢复

7.3.5.1 数据完整性

除满足7.2.5.1的要求之外，还应满足：

a）应能够检测到系统管理数据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的恢复措施；

b）应能够检测到系统管理数据、鉴别信息和重要业务数据在存储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的恢复措施。

7.3.5.2 数据保密性

除满足7.2.5.2的要求之外，还应满足：

a）应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

b）应采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性。

7.3.5.3 备份和恢复

除满足7.2.5.3的要求之外，还应满足：

a）应提供本地数据备份与恢复功能，备份介质场外存放；

b）应提供异地数据备份功能，如利用通信网络将关键数据定时批量传送至备用场地；

c）应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。

7.3.6 物理环境安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中的第3.1级要求。

7.3.7 管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中的第3.1级要求。

7.4 第3.2级要求

7.4.1 业务安全求

除满足7.3.1的要求之外，还应满足：

营业系统、计费系统、账务系统的服务器应当在异址（可为同城不同地点的机房）进行容灾备份，不能出现单点故障。

7.4.2 网络安全

与7.3.2的要求相同。

7.4.3 主机安全

与7.3.3的要求相同。

7.4.4 应用安全

与7.3.4的要求相同。

7.4.5 数据安全及备份恢复

与7.3.5的要求相同。

7.4.6 物理环境安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中的第3.2级要求。

7.4.7 管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中的第3.2级要求。

7.5 第 4 级要求

同第 3.2 级要求。

7.6 第 5 级要求

待补充。

8 支撑网灾难备份及恢复要求

8.1 灾难备份及恢复等级

根据 YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》5.1 节，灾难备份及恢复定级应与安全等级保护确定的安全等级一致。

8.2 第 1 级要求

不作要求。

8.3 第 2 级要求

8.3.1 冗余系统、冗余设备及冗余链路

a）支撑网应具备一定的抗灾难以及灾难恢复能力，重要服务器、重要部件、重要数据库应当采用本地双机备份的方式进行容灾保护；

b）支撑网网络灾难恢复时间应满足行业管理、网络和业务运营商应急预案的相关要求。

8.3.2 数据备份

a）系统的关键数据（如网管系统的配置数据、业务支撑系统的用户资料 、费率表等）应提供本地备份；

b）支撑网的数据备份范围和时间间隔、数据恢复能力应符合行业管理、网络和业务运营商应急预案的相关要求。

8.3.3 人员和技术支持能力

a）支撑网应有安全管理人员和各类技术人员；

b）相关技术人员定期进行灾难备份及恢复方面的技能培训。

8.3.4 运行维护管理能力

a）支撑网应有介质存取、验证和转储管理制度，确保备份数据授权访问；

b）支撑网应按介质特性对备份数据进行定期的有效性验证；

c）支撑网应有相关服务器设备的灾难备份及恢复的管理制度。

8.3.5 灾难恢复预案

a）支撑网应有完整的灾难恢复预案；

b）支撑网应有灾难恢复预案的教育和培训，相关人员应了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力；

c）支撑网应有灾难恢复预案的演练，并根据演练结果对灾难恢复预案进行修正。

8.4 第3.1级要求

8.4.1 冗余系统、冗余设备及冗余链路

与8.3.1的要求相同。

8.4.2 数据备份

与8.3.2的要求相同。

8.4.3 人员和技术支持能力

与8.3.3的要求相同。

8.4.4 运行维护管理能力

与8.3.4的要求相同。

8.4.5 灾难恢复预案

与8.3.5的要求相同。

8.5 第3.2级要求

8.5.1 冗余系统、冗余设备及冗余链路

除满足8.4.1的要求之外，还应满足：

a）支撑网应具备一定的抗灾难以及灾难恢复能力，重要服务器、重要部件、重要数据库应当采用异地机备份的方式进行容灾保护；

b）支撑网应具备冗余链路，关键设备之间应当提供多条物理链路（如计费系统和账务系统之间），以保证通信的不间断。

8.5.2 数据备份

除满足8.4.2的要求之外，还应满足：

系统的关键数据应提供异址备份（可为同城不同地点）。

8.5.3 人员和技术支持能力

与8.4.3的要求相同。

8.5.4 运行维护管理能力

与8.4.4的要求相同。

8.5.5 灾难恢复预案

除满足8.4.5的要求之外，还应满足：

支撑网应有完善的灾难恢复预案管理制度。

8.6 第4级要求

同第3.2级要求。

8.7 第5级要求

待补充。

参 考 文 献

1. 国家标准　　信息安全技术　信息系统安全等级保护基本要求（报批稿）
2. YD/T 1728-2008　电信网和互联网安全防护管理指南