YD

中华人民共和国通信行业标准

YD/T 1758-2008

非核心生产单元安全防护要求

Security Protection Requirements
for the Support Unit of Core Production 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 1759-2008《非核心生产单元安全防护检测要求》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、中国网络通信集团公司、中国电信集团公司、中国移动通信集团公司、中国联合通信有限公司、中国铁通集团有限公司

本标准主要起草人：杨剑锋、刘险峰、赵　阳、陈　欣、顾旻霞、王君珂、张　威

非核心生产单元安全防护要求

1 范围

本标准规定了公众电信网和互联网相关非核心生产单元在安全等级保护、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和互联网相关非核心生产单元。

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 1728-2008　电信网和互联网安全防护管理指南

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 定义和缩略语

3.1 定义

下列定义适用于本标准。

3.1.1

非核心生产单元安全等级 Security Classification of the Support Unit of Core Production Network

非核心生产单元安全重要程度的表征。重要程度可从非核心生产单元受到破坏后，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。

3.1.2

非核心生产单元安全等级保护 Classified Security Protection of the Support Unit of Core Production Network

对非核心生产单元分等级实施安全保护。

3.1.3

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。

3.1.4

非核心生产单元安全风险 Security Risk of the Support Unit of Core Production Network

人为或自然的威胁可能利用非核心生产单元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。

3.1.5

非核心生产单元安全风险评估 Security Risk Assessment of the Support Unit of Core Production Network

指运用科学的方法和手段，系统地分析非核心生产单元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。防范和化解非核心生产单元安全风险，或者将风险控制在可接受的水平，为最大限度地为保障非核心生产单元的安全提供科学依据。

3.1.6

非核心生产单元资产 Asset of the Support Unit of Core Production Network

非核心生产单元中具有价值的资源，是安全防护保护的对象。非核心生产单元中的资产可能是以多种形式存在，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，如非核心生产单元的设备、线路、数据信息等。

3.1.7

非核心生产单元资产价值 Asset Value of the Support Unit of Core Production Network

非核心生产单元中资产的重要程度或敏感程度。非核心生产单元资产价值是非核心生产单元资产的属性，也是进行非核心生产单元资产识别的主要内容。

3.1.8

非核心生产单元威胁 Threat of the Support Unit of Core Production Network

可能导致对非核心生产单元产生危害的不希望事件潜在起因，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。常见的非核心生产单元威胁有攻击、故障、灾害等等。

3.1.9

非核心生产单元脆弱性 Vulnerability of the Support Unit of Core Production Network

脆弱性是非核心生产单元中存在的弱点、缺陷与不足，不直接对非核心生产单元资产造成危害，但可能被非核心生产单元威胁所利用从而危及非核心生产单元资产的安全。

3.1.10

非核心生产单元灾难 Disaster of the Support Unit of Core Production Network

由于各种原因，造成非核心生产单元故障或瘫痪，使非核心生产单元提供的服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。

3.1.11

非核心生产单元灾难备份 Backup for Disaster Recovery of the Support Unit of Core Production Network

为了非核心生产单元灾难恢复而对相关的要素进行备份的过程。

3.1.12

非核心生产单元灾难恢复 Disaster Recovery of the Support Unit of Core Production Network

为了将非核心生产单元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、并将其提供的服务功能、服务水平等，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。

3.2 缩略语

下列缩略语适用于本标准。

DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
FTP	File Transfer Protocol	文件传输协议
HTTP	Hyper Text Transfer Protocol	超文本传输协议
IP	Internet Protocol	网际协议
POP3	Post Office Protocol v3	邮政代理协议第3版
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议

4 非核心生产单元安全防护概述

4.1 非核心生产单元安全防护范围

非核心生产单元通常包括企业办公系统、客服呼叫中心、企业门户网站等。

4.2 非核心生产单元安全防护内容

根据YD/T 1728-2008《电信网和互联网安全防护管理指南》中电信网和互联网安全防护体系的要求，将非核心生产单元安全防护内容分为安全风险评估、安全等级保护、灾难备份及恢复等三个部分：

——非核心生产单元安全等级保护

主要包括定级对象和安全等级的确定、应用安全、网络安全、设备安全、物理环境安全、管理安全等。

——非核心生产单元安全风险评估

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。本标准仅对非核心生产单元进行资产分析、脆弱性分析、威胁分析，在非核心生产单元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》。

——非核心生产单元灾难备份及恢复

主要包括灾难备份及恢复等级确定、针对灾难备份及恢复对各资源要素的具体要求等。

5 非核心生产单元定级对象和安全等级确定

我国电信网、互联网络和业务运营企业非核心生产单元的定级对象通常应为企业办公系统、客服呼叫中心、企业门户网站等。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》附录A中确定安全等级的方法对非核心生产单元定级，即对企业办公系统、客服呼叫中心、企业门户网站等根据社会影响力、所提供服务的重要性、服务规模的大小分别定级，权重α、β、γ可根据具体网络情况进行调节。

6 非核心生产单元资产、脆弱性、威胁分析

6.1 资产分析

非核心生产单元资产的识别与选取应符合科学性、合理性，非核心生产单元资产大致包括各类设备及主机、数据信息、服务、人员、环境设施等。非核心生产单元的资产分析应包括但不限于表1所列范围。

表 1 资产类别

类 别	资 产
设备及主机	各类服务器、终端、辅助设备等；企业网络相关各类路由、交换设备、内部线路，安全过滤、入侵检测和防护设备等
独立软件	包括有必要独立识别的软件，如应用软件、系统程序、数据库等
数据信息	包括内部网络、设备、功能系统相关的各类服务、配置、管理等方面的信息和数据等；内部系统存放和使用的各类文件、资料的信息和数据等
服务	各功能服务系统及其他相关资源提供服务的能力、服务质量等
人员	各类直接服务、维护、管理人员以及相关经验、能力等
环境/设施	包括物理环境，以及电力供应、防火、防水、防静电、温湿度等相关设备设施等

6.2 脆弱性分析

非核心生产单元的脆弱性包括技术脆弱性和管理脆弱性两个方面。脆弱性识别对象应以资产为核心。非核心生产单元的脆弱性分析应包括但不限于表2所列范围。

表 2 脆弱性类别

类 别	对 象	脆弱性
技术脆弱性	系统	包括系统功能规划、部署、资源配置的缺陷等；内部网络保护和恢复能力的缺陷、安全技术措施和策略等方面的漏洞等；相关数据信息在存放、使用、传送、备份、保存、恢复等环节的安全保护技术缺陷和安全策略的漏洞等
	设备	包括各设备、服务器、终端硬件安全性和软件安全性的漏洞等；可靠性、稳定性、业务支持能力和数据处理能力、容错和恢复能力的缺陷等；后台维护和访问相关授权、管理等方面的安全漏洞，以及授权接入的口令、方式、安全连接、用户鉴别、代理等访问控制方面存在的漏洞隐患等
	物理环境	包括物理环境安全防护能力的缺陷；可分为办公场地选择，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制、线路、其他设施及设备的保护等
管理脆弱性		包括相关的方案和预案、人员、保障、组织等安全机制和管理制度在制定和实施等环节的漏洞和缺陷，可分为安全管理机构方面（如岗位设置、授权和审批程序、沟通和合作等），安全管理制度方面（如管理制度及相应的评审和修订等），人员安全管理方面（如人员录用、上岗、安全培训、组织、访问控制等），建设管理方面（如安全方案不完善、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），运维管理方面（如物理环境管理、设备维护、技术支持、关键性能指标监控、攻击防范措施、数据备份和恢复、访问控制、操作管理、应急保障措施等）

6.3 威胁分析

非核心生产单元的威胁根据来源可分为技术威胁、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。非核心生产单元的威胁分析应包括但不限于表3所列范围。

表 3 威胁类别

类 别	威 胁
技术威胁	包括设备相关故障，未充分考虑冗余、可靠性及安全、服务需求等原因，妨碍相关功能完全实现的缺陷或隐患而造成的安全事件等；错误响应和恢复等；相关数据、信息在备份、保存、处理过程中发生的差错、损坏、丢失等；其他突发、异常事件的冲击和数据拥塞等

表3（续）

类 别		威 胁
环境威胁	物理环境	包括供电故障，灰尘、潮湿、温度超标，静电、电磁干扰等；意外事故或线路方面的故障等
	灾害	包括鼠蚁虫害；洪灾、火灾、地震、台风、雷电等自然灾害；战争、社会动乱、恐怖活动等
人为威胁	恶意人员	包括针对相关功能系统的恶意拥塞，针对服务、设备等相关数据和信息的拦截、篡改、删除等攻击行为和恶意扫描、监听、截获等嗅探行为；恶意代码、病毒等；非授权访问、越权操作等；伪造和欺骗等；物理攻击，损坏、盗窃等
	非恶意人员	包括误操作；无作为、技能不足等；相关数据、信息无意泄漏，数据损坏和丢失等；组织、安全管理制度不完善、制度推行不力、缺乏资源等非规范安全管理等

7 非核心生产单元安全等级保护要求

7.1 第1级要求

本标准对安全等级为第1级的非核心生产单元暂不作要求。

7.2 第2级要求

7.2.1 应用安全要求

7.2.1.1 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。

7.2.1.2 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。

7.2.1.3 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。

7.2.1.4 通信数据安全性

a）应采用校验码技术保证通信过程中数据的完整性；

b）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；

c）应采用加密或其他保护措施实现鉴别信息的存储保密性；

d）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；

e） 应对通信过程中的敏感信息进行加密。

7.2.1.5 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。

7.2.2 网络安全要求

7.2.2.1 结构安全

a） 应绘制与当前运行情况相符的网络拓扑结构图；

b） 应根据应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽；

c） 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，按照统一的管理和控制原则划分不同的子网或网段。

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；

d） 应限制具有拨号访问权限的用户数量。

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 入侵防范

a） 应在网络边界处对发生的端口扫描、强力攻击、木马后门攻击、DoS/DDoS 攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击和入侵事件提供有效的抵御和防范能力；

b） 应能够对内部网络中出现的内部用户未通过授权，私自联到外部网络的行为进行检查。

7.2.3 设备安全要求

7.2.3.1 安全检测

a） 应对构建相关系统网络结构的数据网络设备，如各类路由器、交换机等，进行必要的安全检测；相关组网设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定，并应符合网络和业务运营商相关设备的要求；网络设备原则上应符合设备入网管理相关要求的规定；

b） 应对提供相关应用和服务的各类通用计算机、服务器等主机设备进行必要的安全检测，出具安全测试及验收报告并妥善保存；各类计算机、服务器设备应符合并满足网络和业务运营商相关通用设备的要求。

7.2.3.2 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） 通用主机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）当对主机进行远程管理时，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。

7.2.3.3 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。

7.2.3.4 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。

7.2.3.5 恶意代码防范

a）通用主机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，并通过安全的方式（如设置升级服务器）保持系统补丁及时得到更新；

b）通用主机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；

c）通用主机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 物理环境安全要求

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》中第2级的相关要求。

7.2.5 管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的相关要求。

7.3 第3.1级要求

7.3.1 应用安全要求

7.3.1.1 身份鉴别

除满足第2级的要求之外，还应满足：

应能根据需要对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

7.3.1.2 访问控制

除满足第2级的要求之外，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。

7.3.1.3 安全审计

除满足第2级的要求之外，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。

7.3.1.4 通信数据安全性

除满足第2级的要求之外，还应满足：

a） 应采用密码技术保证通信过程中数据的完整性；

b） 应对通信过程中的整个报文或会话过程进行加密；

c） 应能根据需要提供必要的通信数据防抵赖的功能。

7.3.1.5 资源控制

除满足第2级的要求之外，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，并能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。

7.3.2 网络安全要求

7.3.2.1 结构安全

除满足第2级的要求之外，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

除满足第2级的要求之外，还应满足：

a） 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，控制粒度为端口级；

b） 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；

c） 当会话在一定时间内处于非活跃状态或会话结束后应终止网络连接；

d） 应限制网络最大流量数及网络连接数；

e） 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

除满足第2级的要求之外，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 入侵防范

除满足第2级的要求之外，还应满足：

a） 应在网络边界处对恶意代码进行检测和清除；应维护恶意代码库的升级和检测系统的更新；

b） 当检测到入侵行为时，应记录攻击源 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；

c） 应能够对非授权设备私自联到内部网络、以及内部网络用户私自联到外部网络等行为进行检查，准确定出位置，并对其进行有效阻断。

7.3.3 设备安全要求

7.3.3.1 安全检测

同第2级要求。

7.3.3.2 身份鉴别

除满足第2级的要求之外，还应满足：

应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

7.3.3.3 访问控制

除满足第2级的要求之外，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。

7.3.3.4 安全审计

除满足第2级的要求之外，还应满足：

a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

b） 应能够根据日志记录数据进行分析，并生成审计报表；

c） 应保护审计进程，避免受到未预期的中断。

7.3.3.5 恶意代码防范

除满足第2级的要求之外，还应满足：

a） 应能够对重要主机进行入侵行为的监测，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） 通用主机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；

c） 通用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

除满足第2级的要求之外，还应满足：

a） 应对重要主机进行性能监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b） 应能够对服务器、数据库等系统的服务水平设定报警阈值，当监测到服务水平降低到阈值时应能进行报警。

7.3.4 物理环境安全要求

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》中第3.1级的相关要求。

7.3.5 管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第3.1级的相关要求。

7.4 第 3.2 级要求

同第3.1级的要求。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

安全等级为第5级的非核心生产单元安全要求待补充。

8 非核心生产单元灾难备份及恢复要求

8.1 概述

根据YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》，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

本标准对安全等级为第1级的非核心生产单元暂不作要求。

8.3 第2级要求

8.3.1 冗余保护要求

a）设备的处理能力应具备一定的冗余，应满足业务高峰期需要。

b）关键设备的重要部件应采用冗余的方式提供保护。

c）系统关键设备、重要线路应采用设备冗余的保护方式，提供灾难备份和恢复的能力。

8.3.2 数据备份要求

a）应建立对关键数据和重要信息进行备份和恢复的管理和控制机制。

b）对关键数据和重要信息应定期进行备份，保证相关数据和信息及时恢复的能力。

8.3.3 相关人员和技术能力要求

a）非核心生产单元运维应有专职的管理责任人。

b）应有系统和设备操作、维护、管理等相关技术人员。

c）相关管理和技术人员应通过技术培训和考核。

8.3.4 运行维护管理能力要求

a）应具有完善运行维护管理制度，管理制度应涵盖系统运行、设备操作等方面。

b）应按照统一的运行维护要求，对系统进行规范化的维护。

c）应保持与其他部门、外部单位间良好的联络和协作能力。

8.3.5 灾难恢复预案要求

a）应建立相应系统的灾难恢复预案。

b）应对灾难恢复预案的进行教育、培训和演练。

8.4 第3.1级要求

8.4.1 冗余保护要求

除满足第2级的要求之外，还应满足：

a）重要设备、线路应采用冗余热备份的保护方式进行保护。

b）系统应有流量负荷分担设计。

c）提供重要服务的系统应进行系统级备份。

8.4.2 数据备份要求

除满足第2级的要求之外，还应满足：

a）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。

b）重要的数据信息和应用服务系统应采用分布式数据结构。

8.4.3 相关人员和技术能力要求

除满足第2级的要求之外，还应满足：

a）应有专职系统和设备操作、维护、管理等相关技术人员。

b）相关管理和技术人员应定期进行安全技术培训和考核。

8.4.4 运行维护管理能力要求

除满足第2级的要求之外，还应满足：

a）应具有介质存取、验证管理制度，确保数据授权访问。

b）应对备份数据进行定期的完整性、有效性验证。

8.4.5 灾难恢复预案要求

除满足第2级的要求之外，还应满足：

应按照统一的灾难恢复预案管理制度对系统相应的预案进行管理。

8.5 第 3.2 级要求

同第3.1级的要求。

8.6 第 4 级要求

同第3.2级要求。

8.7 第 5 级要求

安全等级为第5级的非核心生产单元安全要求待补充。

参 考 文 献

1. GB/T 18336-2000　信息技术 信息技术安全性评估准则
2. GB/T 19716-2005　信息技术 信息安全管理实用规则
3. GB/T 19715.2-2005　信息技术 信息安全管理指南 第2部分
4. GB17859-1999　计算机信息系统安全等级划分准则