YD

中华人民共和国通信行业标准

YD/T 1756-2008

电信网和互联网管理
安全等级保护要求

Classified Management Security Protection Requirements
for 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。

本标准与YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》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、中国铁通集团有限公司

本标准主要起草人：李　成、魏　薇、杨剑峰、王新峰、陈敏时、曾小辛、张　尼、严　萍

电信网和互联网管理安全等级保护要求

1 范围

本标准规定了公众电信网和互联网的管理安全等级保护要求。

本标准适用于电信网和互联网安全防护体系中的各种网络和系统。

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。

3 术语和定义

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、光电网络，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

泛指由多个计算机网络相互连接而形成的网络，它是在功能和逻辑上组成的大型计算机网络。

3.3

安全等级 Security Classification

安全重要程度的表征。重要程度可从网络受到破坏后，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。

4 管理安全等级保护要求

4.1 第1级要求

不作要求。

4.2 第2级要求

4.2.1 安全管理制度

4.2.1.1 管理制度

a）应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

b）应对安全管理活动中重要的管理内容建立安全管理制度；

c）应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

4.2.1.2 制定和发布

a）应指定或授权专门的部门或人员负责安全管理制度的制定；

b）应组织相关人员对制定的安全管理制度进行论证和审定；

c）应将安全管理制度以某种方式发布到相关人员手中。

4.2.1.3 评审和修订

应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

4.2.2 安全管理机构

4.2.2.1 岗位设置

a）应设立安全主管、安全管理各个方面的负责人岗位，定义各负责人的职责；

b）应设立系统管理人员、网络管理人员、安全管理员岗位，定义各个工作岗位的职责。

4.2.2.2 人员配备

应配备一定数量的系统管理人员、网络管理人员、安全管理员等。

4.2.2.3 授权和审批

a）应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；

b）应针对关键活动建立审批流程，并由批准人签字确认。

4.2.2.4 沟通和合作

a）应加强各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的合作与沟通；

b）应加强与相关外部单位的合作与沟通。

4.2.2.5 审核和检查

应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、数据备份等情况。

4.2.3 人员安全管理

4.2.3.1 人员录用

a）应指定或授权专门的部门或人员负责人员录用；

b）应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；

c）应与从事关键岗位的人员签署保密协议。

4.2.3.2 人员离岗

a）应规范人员离岗过程，及时终止离岗员工的所有访问权限；

b）对于离岗人员，应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c）对于离岗人员，应办理严格的调离手续。

4.2.3.3 人员考核

应定期对各个岗位的人员进行安全技能及安全认知的考核。

4.2.3.4 安全意识教育和培训

a）应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；

b）应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；

c）应制定安全教育和培训计划，对网络安全基础知识、岗位操作规程等进行培训。

4.2.3.5 外部人员访问管理

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

4.2.4 安全建设管理

4.2.4.1 定级

a）应明确网络的边界和安全保护等级；

b）应以书面的形式说明网络确定为某个安全等级的方法和理由；

c）应确保网络的定级结果经过相关部门的批准。

4.2.4.2 安全方案设计

a）应根据网络的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b）应以书面形式描述对网络的安全保护要求、策略和措施等内容，形成网络的安全方案；

c）应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；

d）应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

4.2.4.3 产品采购和使用

a）应确保安全产品采购和使用符合国家的有关规定；

b）应确保密码产品采购和使用符合国家密码主管部门的要求；

c）应指定或授权专门的部门负责产品的采购。

4.2.4.4 自行软件开发

a） 应确保开发环境与实际运行环境物理分开；

b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c） 应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

4.2.4.5 外包软件开发

a）应根据开发需求检测软件质量；

b）应要求开发单位提供软件设计的相关文档和使用指南；

c）应在软件安装之前检测软件包中可能存在的恶意代码。

4.2.4.6 工程实施

a）应指定或授权专门的部门或人员负责工程实施过程的管理；

b）应制定详细的工程实施方案，控制工程实施过程。

4.2.4.7 测试验收

a）应对系统进行安全性测试验收；

b）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

c）应组织相关部门和相关人员对网络测试验收报告进行审定，并签字确认。

4.2.4.8 交付

a）应制定网络交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b）应对负责网络运行维护的技术人员进行相应的技能培训；

c）应确保提供网络建设过程中的文档和指导用户进行网络运行维护的文档。

4.2.4.9 安全服务商的选择

a）应确保安全服务商的选择符合国家的有关规定；

b）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

c）应确保选定的安全服务商提供技术支持和服务承诺，必要时与其签订服务合同。

4.2.4.10 备案

应将网络的定级、属性等资料指定专门的人员或部门负责管理，并控制这些材料的使用。

4.2.5 安全运维管理

4.2.5.1 环境管理

a）应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

b）应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c）应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d）应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。

4.2.5.2 资产管理

a）应编制与网络相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b）应建立资产安全管理制度，规定资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

4.2.5.3 介质管理

a）应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

b）应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；

c）应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；

d）应根据所承载数据和软件的重要程度对介质进行分类和标识管理。

4.2.5.4 设备管理

a）应对网络相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b）应建立基于申报、审批和专人负责的设备安全管理制度，对各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

c）应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

d）应确保信息处理设备必须经过审批才能带离机房或办公地点。

4.2.5.5 网络安全管理

a）应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b）应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

c）应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

d）应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

e）应对网络设备的配置文件进行定期备份；

f）应保证所有与外部系统的连接均得到授权和批准。

4.2.5.6 系统安全管理

a）应根据业务需求和系统安全分析确定系统的访问控制策略；

b）应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；

c）应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；

d）应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；

e）应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；

f）应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

4.2.5.7 恶意代码防范管理

a）应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及从网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

b）应指定专人对网络和主机进行恶意代码检测并保存检测记录；

c）应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

4.2.5.8 密码管理

应使用符合国家密码管理规定的密码技术和产品。

4.2.5.9 变更管理

a）应确认网络中要发生的重要变更，并制定相应的变更方案；

b）网络发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。

4.2.5.10 备份与恢复管理

a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b）应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

4.2.5.11 安全事件处置

a）应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b）应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c）应根据安全事件对本网络产生的影响，对本网络安全事件进行等级划分；

d）应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

4.2.5.12 应急预案管理

a）应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

b）应对相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

4.3 第3.1级要求

4.3.1 安全管理制度

4.3.1.1 管理制度

除满足4.2.1.1的要求之外，还应满足：

a）应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动；

b）应形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。

4.3.1.2 制定和发布

除满足4.2.1.2的要求之外，还应满足：

a）安全管理制度应有统一的格式，并进行版本控制；

b）安全管理制度应通过正式、有效的方式发布；

c）安全管理制度应注明发布范围，并对收发文进行登记。

4.3.1.3 评审和修订

除满足4.2.1.3的要求之外，还应满足：

a）安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；

b）应定期或不定期对安全管理制度进行检查和审定。

4.3.2 安全管理机构

4.3.2.1 岗位设置

除满足4.2.2.1的要求之外，还应满足：

a）应设立安全管理工作的职能部门；

b）应成立指导和管理安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；

c）应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

4.3.2.2 人员配备

除满足4.2.2.2的要求之外，还应满足：

a）应配备专职安全管理员，不可兼任；

b）关键事务岗位应配备多人共同管理。

4.3.2.3 授权和审批

除满足4.2.2.3的要求之外，还应满足：

a）应根据各个部门和岗位的职责明确授权审批事项；

b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；

d）应记录审批过程并保存审批文档。

4.3.2.4 沟通和合作

除满足4.2.2.4的要求之外，还应满足：

a）各类管理人员之间、组织内部机构之间以及网络安全职能部门内部定期或不定期召开协调会议，共同协作处理网络安全问题；

b）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；

c）应聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等。

4.3.2.5 审核和检查

除满足4.2.2.5的要求之外，还应满足：

a）应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

b）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

c）应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

4.3.3 人员安全管理

4.3.3.1 人员录用

除满足4.2.3.1的要求之外，还应满足：

a）应严格规范人员录用过程，对被录用人的资质等进行审查；

b）应签署保密协议；

c）应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

4.3.3.2 人员离岗

除满足4.2.3.2的要求之外，还应满足：

关键岗位人员离岗须承诺调离后的保密义务后方可离开。

4.3.3.3 人员考核

除满足4.2.3.3的要求之外，还应满足：

a）应对关键岗位的人员进行全面、严格的安全审查和技能考核；

b）应对考核结果进行记录并保存。

4.3.3.4 安全意识教育和培训

除满足4.2.3.4的要求之外，还应满足：

a）应对安全责任和惩戒措施进行书面规定；

b）应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划；

c）应对安全教育和培训的情况和结果进行记录并归档保存。

4.3.3.5 外部人员访问管理

除满足4.2.3.5的要求之外，还应满足：

a）应确保在外部人员访问受控区域前先提出书面申请；

b）对外部人员允许访问的区域、网络、设备、信息等内容应进行书面的规定，并按照规定执行。

4.3.4 安全建设管理

4.3.4.1 定级

除满足4.2.4.1的要求之外，还应满足：

a） 应组织相关部门和有关安全技术专家对网络定级结果的合理性和正确性进行论证和审定；

b） 应将网络的定级结果分级上报至全国或地区的主管部门，主管部门对定级结果审批。

4.3.4.2 安全方案设计

除满足4.2.4.2的要求之外，还应满足：

a）应指定和授权专门的部门对网络的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

b）应根据网络的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

c）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

d）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

4.3.4.3 产品采购和使用

除满足4.2.4.3的要求之外，还应满足：

应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

4.3.4.4 自行软件开发

除满足4.2.4.4的要求之外，还应满足：

a）应确保开发人员和测试人员分离，测试数据和测试结果受到控制；

b）应制定代码编写安全规范，要求开发人员参照规范编写代码；

c）应确保对程序资源库的修改、更新、发布进行授权和批准。

4.3.4.5 外包软件开发

与4.2.4.5的要求相同。

4.3.4.6 工程实施

除满足4.2.4.6的要求之外，还应满足：

a）要求工程实施单位能正确地执行安全工程过程；

b）应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

4.3.4.7 测试验收

除满足4.2.4.7的要求之外，还应满足：

a）应委托公正的第三方测试单位对网络进行安全性测试，并出具安全性测试报告；

b）应对系统测试验收的控制方法和人员行为准则进行书面规定；

c）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。

4.3.4.8 交付

除满足4.2.4.8的要求之外，还应满足：

a）应对网络交付的控制方法和人员行为准则进行书面规定；

b）应指定或授权专门的部门负责网络交付的管理工作，并按照管理规定的要求完成交付工作；

c）在网络正式投入使用前，应根据实际情况进行试运行，试运行期间应提供相关应急预防措施；

d）在网络正式投入使用后，应对开发、建设过程中涉及安全要求的配置、口令等内容重新修改、设定。

4.3.4.9 安全服务商的选择

与4.2.4.9的要求相同。

4.3.4.10 备案

除满足4.2.4.10的要求之外，还应满足：

应将网络的安全等级、属性、定级的理由等资料分级上报至全国或地区的主管部门备案。

4.3.4.11 等级测评

a）在网络运行过程中，应至少每年对网络进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；

b）应在网络发生变更时及时对网络进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；

c）应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；

d）应指定或授权专门的部门或人员负责等级测评的管理。

4.3.5 安全运维管理

4.3.5.1 环境管理

除满足4.2.5.1的要求之外，还应满足：

a）应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理。

b）工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件。

4.3.5.2 资产管理

除满足4.2.5.2的要求之外，还应满足：

a）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

b）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

4.3.5.3 介质管理

除满足4.2.5.3的要求之外，还应满足：

a）应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b）应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；

c）应对存储介质的使用过程进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准不得自行销毁；

d）应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

e）应对重要介质中的数据和软件采取加密存储。

4.3.5.4 设备管理

除满足4.2.5.4的要求之外，还应满足：

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。

4.3.5.5 监控管理

a）应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；

b）应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；

c）应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

4.3.5.6 网络安全管理

除满足4.2.5.5的要求之外，还应满足：

a）应实现设备的最小服务配置，并对配置文件进行定期离线备份；

b）应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

c）应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

4.3.5.7 系统安全管理

除满足4.2.5.6的要求之外，还应满足：

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

4.3.5.8 恶意代码防范管理

除满足4.2.5.7的要求之外，还应满足：

应定期检查网络内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

4.3.5.9 密码管理

除满足4.2.5.8的要求之外，还应满足：

应建立密码使用管理制度。

4.3.5.10 变更管理

除满足4.2.5.9的要求之外，还应满足：

a）应建立变更管理制度，变更和变更方案需有评审过程；

b）应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

c）应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

4.3.5.11 备份与恢复管理

除满足4.2.5.10的要求之外，还应满足：

a）应建立备份与恢复管理相关的安全管理制度；

b）应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；

c）应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

4.3.5.12 安全事件处置

除满足4.2.5.11的要求之外，还应满足：

a）应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

b）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

c）对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

4.3.5.13 应急预案管理

除满足4.2.5.12的要求之外，还应满足：

a）应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

b）应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；

c）应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

4.4 第3.2级要求

与第3.1级要求相同。

4.5 第4级要求

同第3.2级要求。

4.6 第5级要求

待补充。

参 考 文 献

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)

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