

ICS 33.040
M 10



中华人民共和国通信行业标准

YD/T 3161-2016

邮件系统安全防护要求

Security protection requirements for the mail system

2016-07-11 发布

2016-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

 3.1 术语和定义.....1

 3.2 缩略语.....2

4 邮件系统安全防护概述.....3

 4.1 邮件系统安全防护范围.....3

 4.2 邮件系统安全风险分析.....3

 4.3 邮件系统安全防护内容.....4

5 邮件系统安全防护要求.....4

 5.1 第1级要求.....4

 5.2 第2级要求.....5

 5.3 第3级要求.....11

 5.4 第4级要求.....14

 5.5 第5级要求.....14

附录A（规范性附录）邮件系统风险分析.....15

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预计如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《固定通信网安全防护检测要求》
7. 《移动通信网安全防护要求》
8. 《移动通信网安全防护检测要求》
9. 《互联网安全防护要求》
10. 《互联网安全防护检测要求》
11. 《增值业务网—消息网安全防护要求》
12. 《增值业务网—消息网安全防护检测要求》
13. 《增值业务网—智能网安全防护要求》
14. 《增值业务网—智能网安全防护检测要求》
15. 《接入网安全防护要求》
16. 《接入网安全防护检测要求》
17. 《传送网安全防护要求》
18. 《传送网安全防护检测要求》
19. 《IP承载网安全防护要求》
20. 《IP承载网安全防护检测要求》
21. 《信令网安全防护要求》
22. 《信令网安全防护检测要求》
23. 《同步网安全防护要求》
24. 《同步网安全防护检测要求》
25. 《支撑网安全防护要求》
26. 《支撑网安全防护检测要求》
27. 《非核心生产单元安全防护要求》
28. 《非核心生产单元安全防护检测要求》
29. 《电信网和互联网物理环境安全等级保护要求》
30. 《电信网和互联网物理环境安全等级保护检测要求》
31. 《电信网和互联网管理安全等级保护要求》
32. 《电信网和互联网管理安全等级保护检测要求》

33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网即时消息业务系统安全防护要求》
42. 《增值业务网即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网应用安全防护要求》
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. 《电信和互联网用户个人电子信息保护通用技术要求和管理工作要求》
62. 《电信和互联网用户个人电子信息保护检测要求》
63. 《互联网接入服务安全防护要求》
64. 《互联网接入服务安全防护检测要求》
65. 《网络交易安全防护要求》
66. 《网络交易安全防护检测要求》
67. 《邮件系统安全防护要求》
68. 《邮件系统安全防护检测要求》（本标准）
69. 《公有云服务安全防护要求》

YD/T 3161-2016

70. 《公有云服务安全防护检测要求》

本标准按照GB/T1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

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：中国信息通信研究院、中国电信集团公司、中国联合网络通信集团有限公司。

本标准主要起草人：李 强、魏 薇、何友斌、苏 鹏、牛 云、姜 楠、刘险峰。

邮件系统安全防护要求

1 范围

本标准规定了邮件系统分安全保护等级的安全防护要求，涉及到业务及应用安全、网络安全、设备及软件系统安全、物理环境安全和管理安全。

本标准适用于公众电信网和互联网中的邮件系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

- 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
- YD/T 2692-2014 电信网和互联网用户个人电子信息保护通用技术要求和
- YD/T 2698-2014 电信网和互联网安全防护基线配置要求及检测要求网络设备
- YD/T 2699-2014 电信网和互联网安全防护基线配置要求及检测要求安全设备
- YD/T 2700-2014 电信网和互联网安全防护基线配置要求及检测要求数据库
- YD/T 2701-2014 电信网和互联网安全防护基线配置要求及检测要求操作系统
- YD/T 2702-2014 电信网和互联网安全防护基线配置要求及检测要求中间件
- YD/T 2703-2014 电信网和互联网安全防护基线配置要求及检测要求WEB应用系统

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

邮件系统安全等级 Security Classification of Mail System

邮件系统安全重要程度的表征。重要程度可从邮件系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、业务运营企业造成的损害来衡量。

3.1.2

邮件系统安全等级保护 Classified Security Protection of Mail System

对邮件系统分等级实施安全保护。

3.1.3

邮件系统安全风险 Security Risk of Mail System

人为或自然的威胁可能利用邮件系统中存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

邮件系统资产 Asset of Mail System

YD/T 3161-2016

邮件系统中具有价值的资源，是安全防护保护的对象。邮件系统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，如邮件系统的主机、网络布局等。

3.1.5

邮件系统威胁 Threat of Mail System

可能导致对邮件系统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。常见的邮件系统威胁有光缆中断、设备节点失效、火灾、水灾、垃圾邮件、邮件病毒、钓鱼邮件、拒绝服务攻击等。

3.1.6

邮件系统脆弱性 Vulnerability of Mail System

邮件系统中存在的弱点、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及资产的安全。

3.1.7

邮件系统灾难 Disaster of Mail System

由于各种原因，造成邮件系统故障或瘫痪，使邮件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。

3.1.8

邮件系统灾难备份 Backup for Disaster Recovery of Mail System

为了邮件系统灾难恢复而对相关网络要素进行备份的过程。

3.1.9

邮件系统灾难恢复 Disaster Recovery of Mail System

为了将邮件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。

3.1.10

业务使用用户 Business Users

注册邮件、使用邮件的用户。

3.1.11

后台管理用户 Manage Users

对邮件系统进行日常运维的后台管理用户。

3.1.12

客户端 Client

登陆邮件系统的客户端软件，包括邮件系统自开发客户端和第三方客户端。

3.2 缩略语

下列缩略语适用于本文件。

DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务

IMAP	Internet Mail Access Protocol	互联网邮件访问协议
POP	Post Office Protocol	邮局协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议

4 邮件系统安全防护概述

4.1 邮件系统安全防护范围

邮件系统是指通过互联网建立采用邮件简单传输协议(SMTP)、邮局协议(POP)、邮件访问协议(IMAP)等为用户提供一对一、一对多的邮件编辑、发送、传输、接收、存储、转发的电子信箱业务系统。它利用智能终端、计算机等与互联网结合，通过存储转发方式为用户提供多种类型的信息交换。

邮件系统整体架构包含以下几个关键模块：

- 1) 注册登录模块：为新用户提供注册和已注册用户提供服务；
- 2) 业务处理模块：为注册用户接收邮件、发送邮件的服务；
- 3) 数据存储模块：为注册用户邮件数据存储服务；
- 4) 业务安全管理模块：为注册用户恶意代码监控和过滤服务；
- 5) 系统安全管理模块：设备配置管理和设备运行状态监控，确保系统运行稳定。

邮件系统功能架构如图1所示。

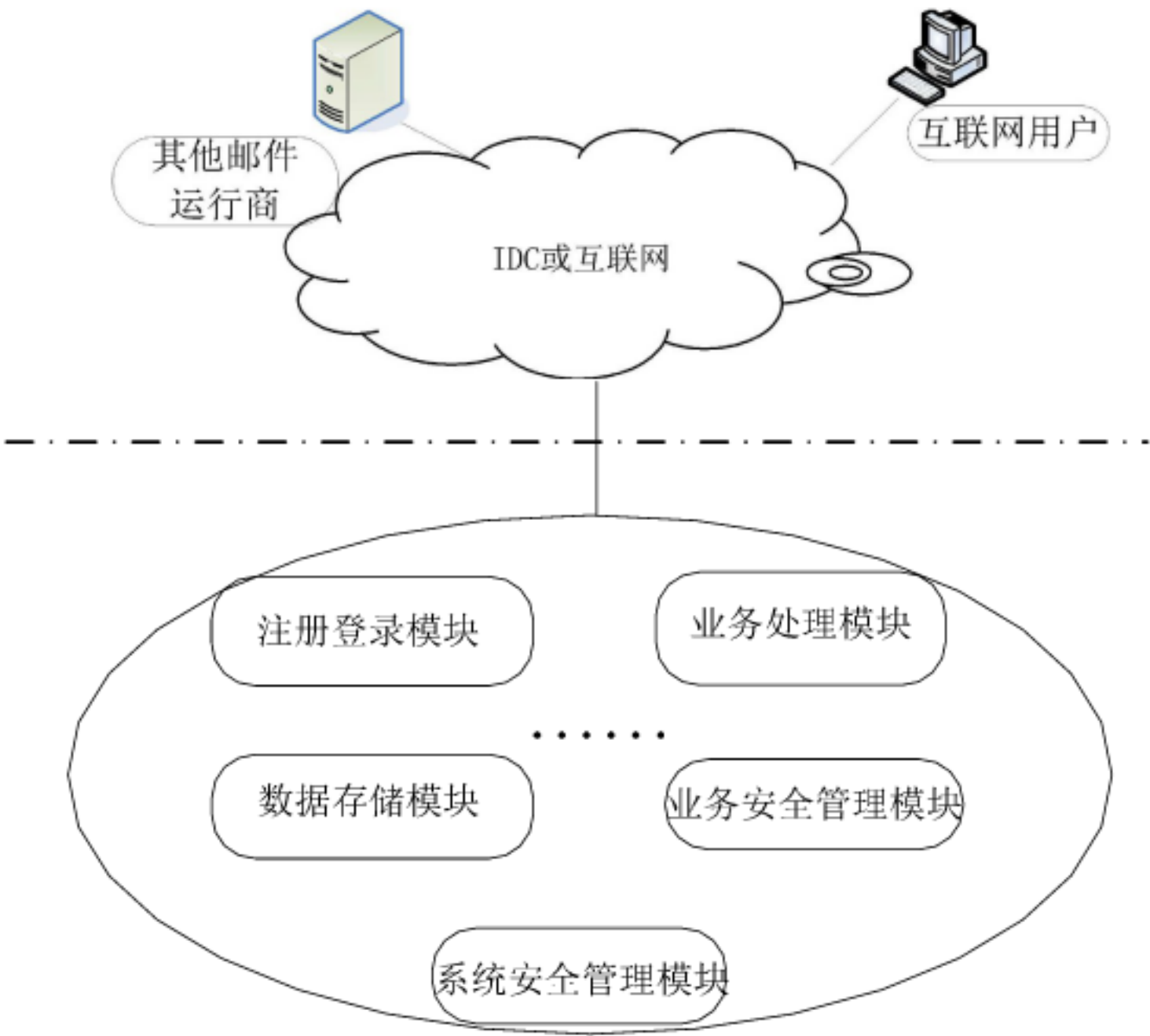


图1 邮件系统功能架构

4.2 邮件系统安全风险分析

邮件系统的重要资产至少应包括：

- 1) 邮件系统及操作维护终端：如注册登录模块、业务处理模块、数据存储模块、业务安全管理模块及系统安全管理模块等涉及的服务器、数据库和操作维护终端；系统内部网络设备(如系统内部组网路由器、交换机等)、系统内部链路等；

YD/T 3161-2016

2) 邮件关键数据：如用户邮件注册信息（用户名、口令等）、用户邮件数据内容、邮件系统服务器的后台管理账户、口令等。

邮件系统的资产类别应包括但不限于附录A表A.1所列范围。

邮件系统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。邮件系统的脆弱性分析应包括但不限于附录A表A.2所列范围。

邮件系统的威胁根据来源可分为环境威胁、技术威胁和人为威胁。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。邮件系统的威胁分析应包括但不限于附录A表A.3所列范围。

邮件系统面临来自公众互联网和内部网络的各种安全威胁，其最突出安全风险是邮件系统收发服务的可用性和用户敏感数据信息泄露，包括：

- 1) 邮件系统故障或瘫痪，造成业务持续性中断；
- 2) 邮件内容泄露；
- 3) 邮箱登录用户名和口令被他人非法获取；
- 4) 含恶意代码的邮件（图片、文档、视频、音频等）被恶意传播；
- 5) 垃圾邮件被大量发送。

这些安全隐患会对邮件系统及时、准确地提供邮件收发服务构成威胁，甚至进一步威胁基础网络和互联网用户终端的安全。

4.3 邮件系统安全防护内容

邮件系统的主要功能是为用户提供邮件的写、发、收、存服务，因此保障其业务及应用系统安全运行，防止用户敏感数据泄露至关重要。保障邮件系统网络安全、设备及软件系统安全、管理安全等也是安全防护的主要内容。邮件系统安全防护的内容具体包括：

- 1) 业务及应用安全。业务及应用安全包括身份鉴别、访问控制、安全审计、数据安全、资源控制、信息保护、Web安全防护、客户端安全、对外能力接口安全、恶意代码防范等方面安全要求。
- 2) 网络安全。网络安全包括网络结构安全、入侵防范、安全审计等方面安全要求。
- 3) 设备及软件系统安全。设备及软件系统安全包括网络及安全设备、操作系统、数据库、中间件等方面安全要求。
- 4) 物理环境安全。物理环境安全包括物理机房位置、机房访问控制等方面的安全要求。
- 5) 管理安全。管理安全包括安全管理制度、机构、人员等方面的安全要求。

5 邮件系统安全防护要求

5.1 第1级要求

5.1.1 业务及应用安全

5.1.1.1 身份鉴别

应提供专用的登录控制模块对登录系统的业务使用用户进行身份标识和鉴别。

5.1.1.2 访问控制

应提供业务使用用户、后台管理用户访问控制功能。

5.1.1.3 信息保护

应满足YD/T 2692-2014《电信网和互联网用户个人电子信息保护通用技术要求和管

5.1.1.4 Web安全

应满足YD/T 2703-2014《电信网和互联网安全防护基线配置要求及检测要求 Web应用系统》要求。

5.1.1.5 对外接口安全

应提供数据有效性检验功能，保证通过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。

5.1.2 网络安全

5.1.2.1 网络结构

应绘制与当前运行情况相符的系统拓扑结构图。

5.1.2.2 网络监测

应在系统边界部署访问安全监测设备，并启用有效的安全监测控制策略。

5.1.2.3 安全审计

应对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少180天）。

5.1.3 设备及软件系统安全

5.1.3.1 网络及安全设备

网络及安全设备应符合以下要求：

- a) 各类路由器、交换机等网络设备应满足相关通信行业标准要求，具有进网许可证；
- b) 应满足YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求网络设备》要求；
- c) 应满足YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求安全设备》要求。

5.1.3.2 通用主机操作系统

通用主机操作系统应符合以下要求：

- a) 应满足YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求操作系统》要求；
- b) 各个功能模块的计算机运维终端、服务器等设备的审计范围应覆盖到主机/服务器上的每个操作系统用户。

5.1.3.3 数据库及中间件软件

数据库及中间件软件应符合以下要求：

- a) 应满足YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求中间件》要求；
- b) 应满足YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求数据库》要求；
- c) 邮件系统中各个功能模块的数据库及中间件软件的审计范围应覆盖到每个数据库及中间件软件用户。

5.2 第2级要求

5.2.1 业务及应用安全

5.2.1.1 身份鉴别

除满足第1级的要求之外，还应提供并启用业务使用用户身份标识唯一性检查的功能，保证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。

5.2.1.2 访问控制

访问控制应符合以下要求：

a) 应提供访问控制功能，依据安全策略控制业务使用用户、后台管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户；

b) 应提供并启用业务使用用户登录认证策略，如防范暴力破解、防范暴力获取用户名、限定失败登录次数、锁定时间等；

c) 应在屏蔽带病毒网页后，为用户发送消息提示。

5.2.1.3 安全审计

安全审计应符合以下要求：

a) 应提供覆盖到系统每一个业务使用用户、后台管理用户的安全审计功能，至少应能对用户关键操作、重要行为、系统重要安全事件等进行审计；

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。

5.2.1.4 数据安全性

数据安全性应符合以下要求：

a) 应提供用户登录认证过程的数据加密传输功能；

b) 应对邮件内容进行数据保护，采取非明文存储方式；

c) 应防范和过滤垃圾邮件，保证用户邮件的正常使用；

d) 应对进入邮件服务器的邮件（如发送地址、接收地址、标题等）是否包含恶意链接及恶意代码进行必要的检测，并对邮件收发地址有效性进行验证。

5.2.1.5 资源控制

资源控制应符合以下要求：

a) 登录用户在超过限定时间内未作任何操作，系统应该自动登出；

b) 应能够对同类型登录设备中单个用户的多重并发会话进行限制。

5.2.1.6 信息保护

信息保护应符合以下要求：

a) 在获取业务使用用户信息时，应采取传输加密等措施保障相应数据的传输安全；

b) 应采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储设备的安全；

c) 应妥善保存用户信息数据的纸质资料、电子介质等；

d) 在用户申请、审核及投诉处理过程中使用用户数据信息外，不得将用户数据信息用于任何其他用途；

e) 应采取措施加强对接触到用户数据信息人员的管理，严格控制接触用户信息的人员范围，合理设定用户信息操作权限，防止出现人为信息泄漏事件；

f) 应当明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人，利用该信息牟利。在与用户签署的相关合同协议中，应明确规定运营企业对用户信息安全承担保护责任，写明采取的具体信息保护措施；

g) 应对用户信息安全防护工作进行定期检查或抽查，发现有违规行为时，可以依据相关协议等追究其责任。

5.2.1.7 Web 安全

Web安全应符合以下要求：

- a) 应对所有来源输入进行验证并尽量使用白名单验证方法；
- b) 应设计一套统一的验证接口，向整个应用系统提供一致的验证方法；
- c) 应在服务器端进行输入验证，避免客户端输入验证被绕过；
- d) 应对输入内容进行规范化处理后再进行验证，如文件路径、URL地址等；
- e) 应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权；
- f) 应采用统一的访问控制机制，保证整体访问控制策略的一致性，同时应确保访问控制策略不被非法修改；
- g) 应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，新创建的会话标识应满足随机性和长度要求，避免被攻击者猜测（如采用会话与IP地址绑定的方式），降低会话被盗用的风险；
- h) 应确保会话数据的存储和传输安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问，当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改；
- i) 应确保会话的安全终止，当用户登录成功并成功创建会话后，应在Web应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话；
- j) 应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息；
- k) 在涉及到关键业务操作的Web页面，应为提供保障会话安全的补充机制（如以Web页面一次性随机令牌的方式，作为主会话标识的补充）。

5.2.1.8 客户端安全

客户端安全应符合以下要求：

- a) 客户端应对输入数据做严格验证；
- b) 客户端应确保身份认证模块不能被非法绕过；
- c) 客户端软件运行时应对自身进行完整性校验，及时有效的发现是否被恶意修改；
- d) 客户端应采取会话保护措施防止软件与服务器之间的会话被篡改、伪造、重放等；
- e) 客户端应确保软件配置信息、用户认证信息、本地存储的用户邮件信息等敏感数据采用加密方式存储；
- f) 客户端软件应具有异常处理功能。

5.2.1.9 对外接口安全

对外接口安全应符合以下要求：

- a) 接口均应分别设置专门前置服务器，通过前置服务器的接口应用实现内外系统的交互；
- b) 接口数据传输应尽量采用加密方式，原则上要求内外系统交互时，接口报文中的敏感信息应进行加密传输，如接口认证需要的密码等敏感数据；

- c) 接口数据传输应进行校验，确保数据在传输过程中的完整性；
- d) 接口认证信息应以密文的形式单独存储在配置文件中；

5.2.2 网络安全

5.2.2.1 网络结构

除满足第1级的要求之外，还应根据自身应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽。

5.2.2.2 网络监测

网络监测应符合以下要求：

- a) 应在系统边界部署访问安全监测设备，并启用有效的安全监测控制策略；
- b) 应具备恶意代码监测功能，对通过该平台对外发布的信息使用自动程序过滤和人工检查结合的方式进行恶意代码监测、检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播；
- c) 各个功能模块的计算机运维终端、服务器等设备应安装病毒、木马等恶意代码的监测和查杀软件，并能对监测日志进行实时备份，以及定期更新防恶意代码软件版本和恶意代码库；
- d) 各个功能模块的计算机运维终端、服务器等设备应支持防恶意代码监测和查杀软件的统一管理。

5.2.2.3 安全审计

除满足第1级的要求之外，还应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。

5.2.3 设备及软件系统安全

5.2.3.1 网络及安全设备

网络及安全设备应符合以下要求：

- a) 应对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别；
- b) 网络及安全设备管理用户的标识应唯一。

5.2.3.2 通用主机操作系统

5.2.3.2.1 安全检测

安全检测应符合以下要求：

- a) 应对邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统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，相关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；
- b) 各个功能模块的计算机运维终端、服务器等设备的主机操作系统应定期进行安全检测，发现并加固操作系统相关漏洞，避免已发现的漏洞造成安全事件。

5.2.3.2.2 身份鉴别

当对各类主机进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

5.2.3.2.3 访问控制

访问控制应符合以下要求：

- a) 各个功能模块的计算机运维终端、服务器等设备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) 各个功能模块的计算机运维终端、服务器等设备应及时删除多余的、过期的账户，避免共享账户的存在；

c) 各个功能模块的计算机运维终端、服务器等设备应实现操作系统和数据库系统特权用户的权限分离；

d) 各个功能模块的计算机运维终端、服务器等设备应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

5.2.3.2.4 安全审计

安全审计应符合以下要求：

a) 各个功能模块的计算机运维终端、服务器等设备的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；

b) 各个功能模块的计算机运维终端、服务器等设备的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。

5.2.3.2.5 资源控制

资源控制应符合以下要求：

a) 各个功能模块的服务器应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；

b) 各个功能模块的服务器应根据安全策略设置计算机运维终端的操作超时断开链接。

5.2.3.2.6 冗余备份

邮件系统中各个功能模块的服务器应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

5.2.3.3 数据库及中间件软件

5.2.3.3.1 安全检测

安全检测应符合以下要求：

a) 应对邮件系统中各个功能模块的数据库及中间件软件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，相关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；

b) 应对邮件系统中各个功能模块的数据库及中间件软件应定期进行安全检测，发现并加固数据库及中间件软件的相关漏洞，避免已发现的漏洞造成安全事件。

5.2.3.3.2 身份鉴别

身份鉴别应符合以下要求：

a) 在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限；

b) 使用数据库角色来管理对象的权限。

5.2.3.3.3 访问控制

访问控制应符合以下要求：

a) 邮件各个功能模块的数据库及中间件软件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) 各个功能模块的数据库及中间件软件应实现数据库、中间件特权用户与操作系统的权限分离。

5.2.3.3.4 安全审计

安全审计应符合以下要求：

a) 各个功能模块的数据库及中间件软件的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；

b) 各个功能模块的数据库及中间件软件的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。

5.2.3.3.5 资源控制

资源控制应符合以下要求：

a) 各个功能模块的数据库及中间件软件应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；

b) 各个功能模块的数据库及中间件软件应根据安全策略设置计算机运维终端的操作超时锁定。

5.2.3.3.6 冗余备份

各个功能模块的数据库及中间件软件应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

5.2.4 物理环境安全要求

应满足 YD/T 1754-2008 中的第 2 级要求。

5.2.5 管理安全要求

除满足 YD/T 1756-2008 中的第 2 级要求外，还应该满足以下要求。

5.2.5.1 安全管理要求

安全管理应符合以下要求：

a) 至少覆盖但不限于安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等管理方面；

b) 在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，应符合最严格的安全要求。

5.2.5.2 人员和技术支持能力

人员和技术支持能力应符合以下要求：

a) 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。

5.2.5.3 运行维护管理能力

运行维护管理能力应符合以下要求：

a) 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) 应按介质特性对备份数据进行定期的有效性验证；

c) 应有相关服务器设备的灾难备份及恢复的管理制度。

5.2.5.4 风险评估要求

风险评估应符合以下要求：

a) 邮件系统及其所属各类设备、系统应根据安全防护相关规定定期进行安全风险评估（至少每两年一次）；

b) 安全风险评估至少应覆盖业务及应用安全、网络安全、设备及软件系统安全、物理环境安全、管理安全等相关技术风险和人员安全、运维安全等相关管理风险。

5.2.5.5 灾难恢复预案

灾难恢复预案应符合以下要求：

- a) 应按照YD/T 1731-2008的相关要求制定完整的灾难恢复预案及对应管理制度；
- b) 应有灾难恢复预案的教育和培训（至少每半年一次），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) 应有灾难恢复预案的演练（至少每年一次），并根据演练结果对灾难恢复预案进行修正。

5.3 第3级要求

5.3.1 业务及应用安全

5.3.1.1 身份鉴别

除满足第2级的要求之外，还应提供并启用用户登录认证口令复杂度强度功能，保证业务使用用户的口令长度不小于8位，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符组合，且与用户名或身份标识无相关性）并提示用户定期更换。

5.3.1.2 访问控制

除满足第2级的要求之外，还应严格设置业务使用用户解锁策略，按安全策略要求，被锁定的业务使用用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定。

5.3.1.3 安全审计

除满足第2级的要求之外，还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。

5.3.1.4 数据安全性

除满足第2级的要求之外，还应满足：

- a) 应采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改；
- b) 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符合系统设定要求，确保非常规数据被过滤；
- c) 应对邮件内容进行数据保护，采取非明文存储方式，确保加密或者编码算法符合国家商用密码管理办法的相关要求。

5.3.1.5 信息保护

除满足第2级的要求之外，还应保护系统服务相关信息的安全，避免有关数据被篡改和破坏。

5.3.1.6 Web 安全

除满足第2级的要求之外，还应在Web程序上线前或升级后进行代码审计，形成报告，并对审计出的问题进行代码升级完善。

5.3.1.7 客户端安全

除满足第2级的要求之外，还应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考CVE、CNVD等）。

5.3.1.8 对外接口安全

同第2级要求。

5.3.2 网络安全

5.3.2.1 网络结构安全

网络结构安全应符合以下要求：

- a) 应根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署；
- b) 不考虑主动宕机维护的情况，可靠性应达到99%以上；
- c) 应具备必要的流量负荷分担设计。

5.3.2.2 网络监测

网络监测应符合以下要求：

- a) 应监测并禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件；
- b) 应在系统边界处对发生的网络入侵行为（包括但不限于强力攻击、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）提供有效的监测能力。当监测到入侵行为时应能立即断开入侵者与主机之间的连接，向管理人员发出警报，并记录攻击源IP、攻击类型、攻击目的、攻击时间。

5.3.2.3 安全审计

除满足第2级的要求之外，还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。

5.3.3 设备及软件操作系统安全

5.3.3.1 网络及安全设备

网络及安全设备应符合以下要求：

- a) 网络及安全设备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；
- b) 网络及安全设备应通过设定终端接入方式、网络地址范围等条件限制管理终端登录；
- c) 网络及安全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。

5.3.3.2 通用主机操作系统

5.3.3.2.1 安全检测

同第2级要求。

5.3.3.2.2 身份鉴别

身份鉴别应符合以下要求：

- a) 各个功能模块的计算机运维终端、服务器等设备的主机操作系统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；
- b) 各个功能模块的计算机运维终端、服务器等设备进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

5.3.3.2.3 访问控制

同第2级要求。

5.3.3.2.4 安全审计

除满足第2级的要求之外，还应保留各个功能模块的计算机运维终端、服务器等设备的审计记录，避免其受到未预期的删除、修改或覆盖等，保留期限至少180天。

5.3.3.2.5 资源控制

除满足第2级的要求之外，还应能够对各个模块的服务器进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议，并设定阈值，在监测到服务水平降低到阈值时进行报警。

5.3.3.2.6 冗余备份

冗余备份应符合以下要求：

- a) 各个功能模块的服务器应对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份，并建立恢复的管理和控制机制；
- b) 相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

5.3.3.3 数据库及中间件软件

5.3.3.3.1 安全检测

同第2级要求。

5.3.3.3.2 身份鉴别

身份鉴别应符合以下要求：

- a) 应对邮件系统中各个功能模块的数据库及中间件软件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；
- b) 应对邮件系统中各个功能模块的数据库及中间件软件进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

5.3.3.3.3 访问控制

同第2级要求。

5.3.3.3.4 安全审计

除满足第2级的要求之外，还应保留各个功能模块的数据库及中间件软件的审计记录，避免其受到未预期的删除、修改或覆盖等，保留期限至少180天。

5.3.3.3.5 资源控制

除满足第2级的要求之外，还应对各个功能模块的数据库及中间件软件进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议，并设定阈值，在监测到服务水平降低到阈值时进行报警。

5.3.3.3.6 冗余备份

冗余备份应符合以下要求：

- a) 各个功能模块的数据库及中间件软件应对关键数据（如配置数据、管理员操作维护记录、用户信息等）和重要信息进行异址（同城不同地点的机房或异地）备份，并建立恢复的管理和控制机制；
- b) 各个功能模块的数据库及中间件软件中相关数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

5.3.4 物理环境安全要求

应满足第2级要求和YD/T 1754-2008中第3.1级的相关要求。

5.3.5 管理安全要求

管理安全应符合以下要求：

- a) 应满足第2级要求和YD/T 1756-2008中第3.1级的相关要求；

b) 应设有专职的操作、维护技术人员和安全管理人員，应定期组织对相关人员进行技术培训和考核；

c) 灾难恢复预案应按照安全管理制度相关的制修订要求进行管理。

5.4 第4级要求

待定。

5.5 第5级要求

待定。

附 录 A
(规范性附录)
邮件系统风险分析

本附录给出了邮件系统风险分析过程中可用于资产、脆弱性、威胁识别和分析的分类方法。

A.1 资产分析

邮件系统资产的识别与选取应符合科学性、合理性，邮件系统资产主要包括各类设备、主机、数据信息、业务、文件、人员、物理环境设施等。邮件系统的资产类别应包括但不限于表A.1所列范围。

表 A.1 资产类别

类别	主要资产
设备及链路	注册登录模块、收发邮件模块、数据存储模块、安全管理模块等涉及的操作维护终端、服务器和数据库，系统内部网络设备（如系统内部组网路由器、交换机等）、系统内部链路
软件	数据库软件、中间件、业务控制和运维管理软件等
数据和信息	保证系统正常提供业务的数据和信息（如用户邮件注册信息、用户邮件数据内容、邮件系统服务器管理账户、口令等）
文档和资料	纸质以及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）
人员	相关管理、维护、开发、数据备份人员等
环境和设施	业务系统和设备所处的物理环境（如机房、电力、防火、防水、防静电、温湿度控制等相关设施）

A.2 脆弱性分析

邮件系统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。邮件系统的脆弱性分析应包括但不限于表A.2所列范围。

表 A.2 脆弱性类别

类别	对象	主要脆弱性
技术脆弱性	业务及应用	相关服务器未进行合理备份，重要数据未及时进行备份； 相关业务存在逻辑漏洞，相关业务应用系统的代码存在漏洞、后门； 相关服务器开放了不必要的端口； 相关服务器配置不合理，访问控制策略设置不合理； 相关服务器的日志功能没有启用或日志记录不完整； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关口令设置不合理、复杂度不够、或没有定期更新； 设备重要部件未进行合理冗余； 相关设备超过使用年限或核心部件老化； 相关设备发生故障后未及时告警
	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、相关服务器、主机等设备的保护不符合规范

表A.2 (续)

类别	对象	主要脆弱性
管理脆弱性		<p>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；</p> <p>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；</p> <p>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、对于第三方人员未进行限制访问等；</p> <p>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；</p> <p>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，灾难恢复预案不完善</p>

A.3 威胁分析

邮件系统的威胁根据来源可分为环境威胁、技术威胁和人为威胁。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。邮件系统的威胁分析应包括但不限于表A.3所列范围。

表 A.3 威胁类别

类别	主要威胁
环境威胁	<p>物理环境：断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等；意外事故或通讯线路方面的故障</p> <p>自然灾害：鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击</p>
技术威胁	<p>设备失效</p> <p>设备故障</p> <p>饱和的信息系统</p> <p>软件故障</p> <p>需要继续完善</p>
人为威胁	<p>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； 攻击者利用非法手段进入机房内部盗窃、破坏、篡改源站内容，攻击者非法物理访问相关设备、存储介质等； 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源； 攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据； 攻击者利用应用系统扩散病毒、蠕虫，利用相关攻击工具恶意消耗应用系统资源（如DDoS攻击），导致系统能力下降或瘫痪、无法正常提供应用服务； 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失 </p> <p>非恶意人员： 内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作、或无意地执行了错误或危险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； 内部人员由于安全检查不及时不到位导致系统主机(如服务器、网络设备等)使用时间过长或质量问题等导致硬件故障，系统链路发生故障，相关设备的操作系统软件、应用软件运行故障，相关设备数据丢失或系统运行中断，存储介质老化或质量问题等导致不可用，系统不能正常运行 </p>