XX 公司

××项目

安全设计方案

（模板）

<备注：模板中斜体部分用于指导用户填写内容，在采用该模板完成交付物时，需要删除所有斜体内容 >

XX 公司

二〇一 X 年 X 月

批　　准：

审　　核：

校　　核：

编　　写：

版本记录

版本编号	版本日期	说　　明	编制人	审批人

目　录

1 编写依据

《信息系统安全等级保护基本要求》 GB/T22239-2008

《信息技术安全 信息系统等级保护安全设计技术要求》 GB/T 25070-2010

《涉及国家秘密的信息系统分级保护技术要求》 BMB17-2006

《IT 主流设备安全基线技术规范》 （Q/CSG 11804-2010）

《信息系统应用开发安全技术规范》 （Q/CSG 11805-2011）

2 安全需求说明

2.1 风险分析

此处依据安全需求分析报告描述互联网应用系统面临的威胁和脆弱性

2.2 数据安全需求

此处依据安全需求分析报告描述互联网应用系统的数据安全需求，包括：访问控制、机密性、完整性、可用性、不可否认性。按照数据的生命周期（产生、传输、处理、使用、存储、删除）进行描述

2.3 运行安全需求

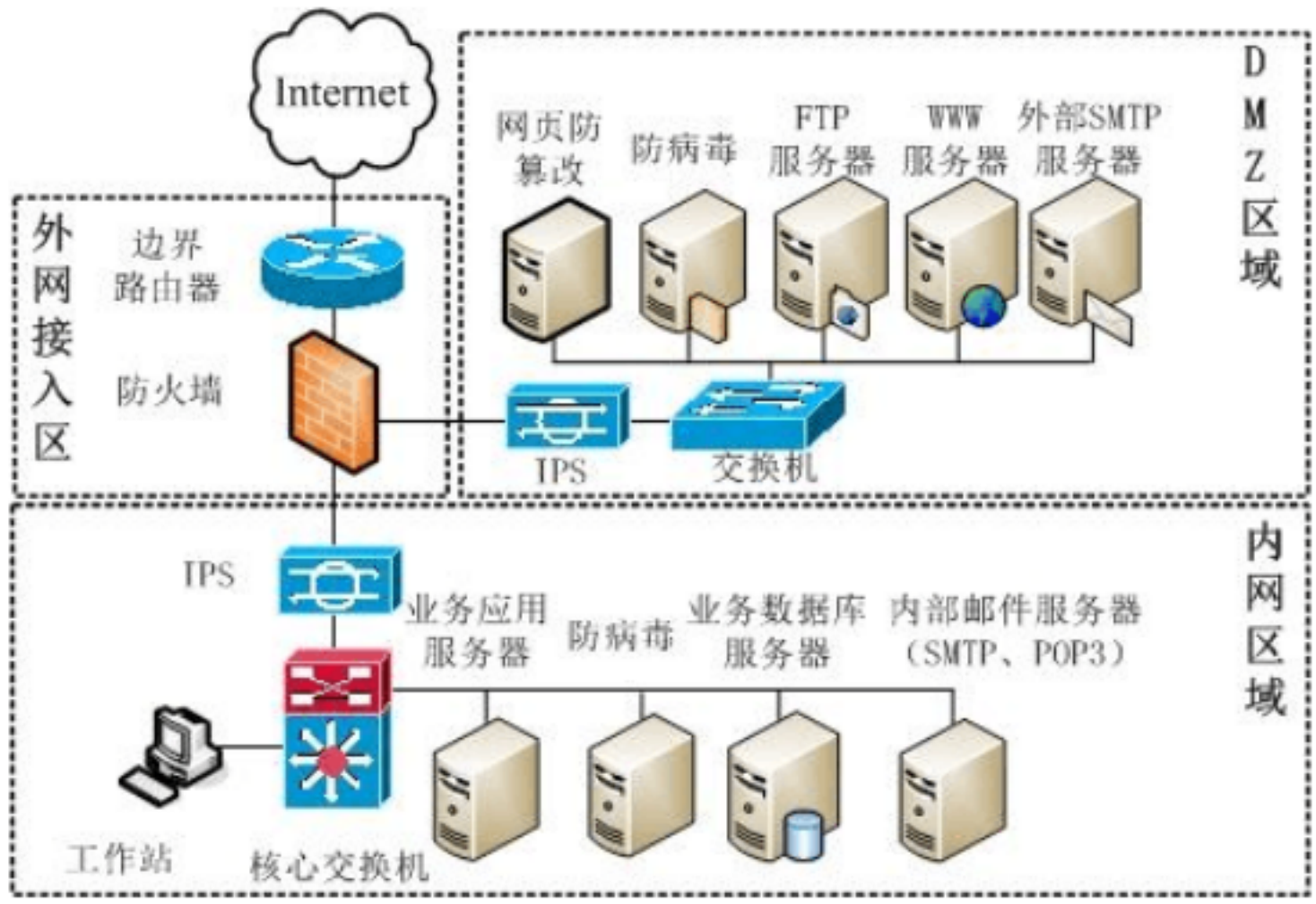
此处依据安全需求分析报告描述互联网应用系统的运行安全需求，包括：安全监控、安全审计、边界安全保护、备份与故障恢复、恶意代码防护

3 系统结构及部署

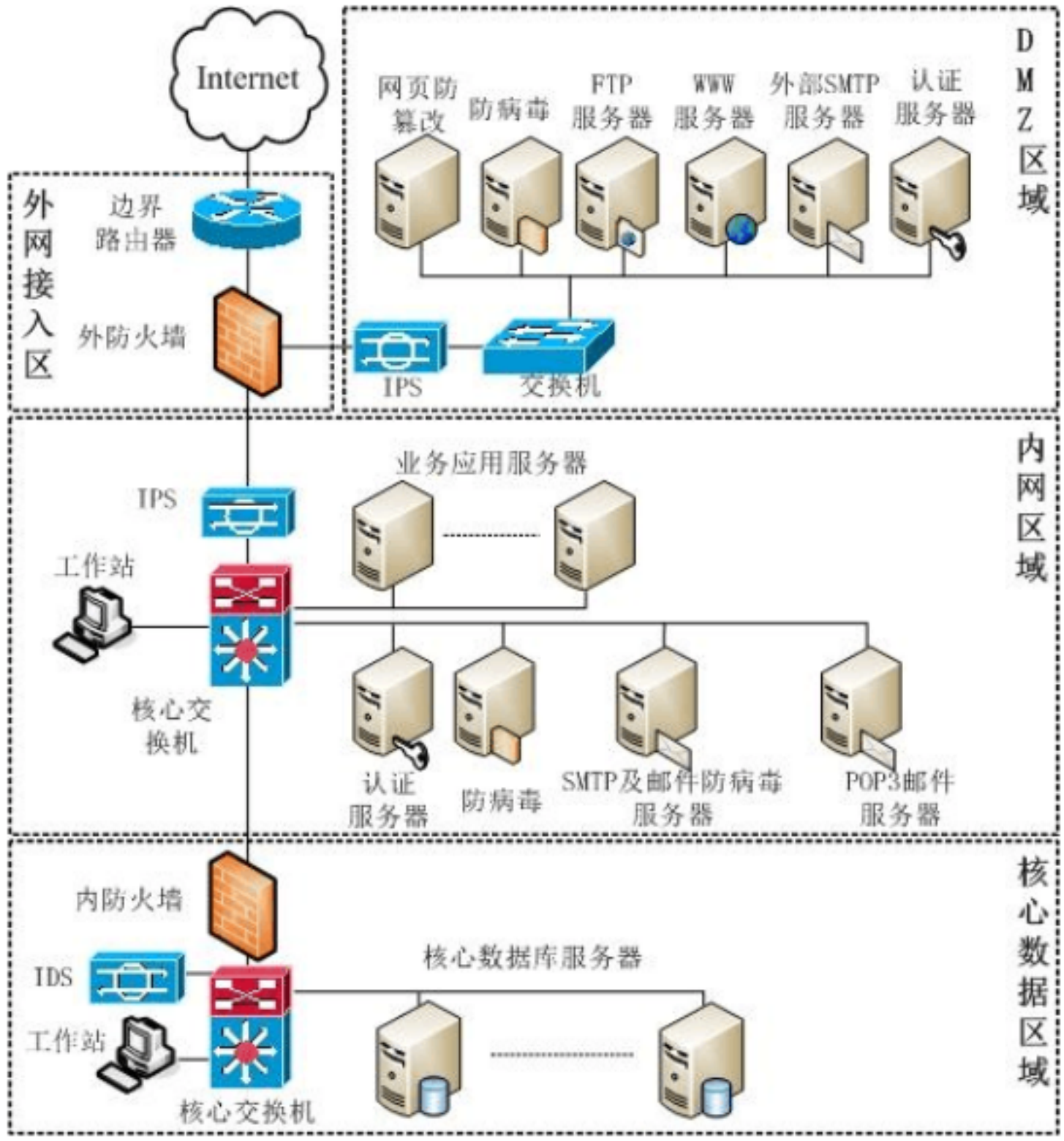
3.1 系统拓扑图

此处描述系统各层设备的部署，主要侧重安全设备之外的设备，包括：

WEB 服务器、应用服务器、数据库服务器 ， 及其所处的区域，包括：外网接入区域、 DMZ 区域、内网区域、核心数据区域、测试区域，示例如下：



二级系统安全需求网络拓扑结构示例



三级系统安全需求网络拓扑结构示例

3.2 负载均衡设计（可选）

此处描述系统具体采用的负载均衡产品型号及数量，部署位置，部署目的，主要的配置策略

3.3 网络存储设计（可选）

此处以系统网络存储设计要求，包括： SAN和 NAS的选择，磁盘阵列的位置要求

3.4 冗余设计（可选）

此处以系统冗余设计要求，包括：单点故障的防范、主备设计、负载均衡

3.5 灾难备份设计（可选）

此处以系统灾难备份设计要求，包括：同城和异地的灾难备份系统建设的要求，网络结构的设计、备份系统设计同步

4 系统安全设计

4.1 网络安全设计

4.1.1 访问控制设计

此处描述系统采用的防火墙的配置策略，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括防火墙的部署、以网段为粒度的访问控制策略、以用户为粒度的网络资源访问控制策略、拨号访问的限制策略。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，根据等保三级要求还需采用的技术设计，包括对应用层协议的过滤控制策略、对超时会话的终止控制策略、对网络最大流量数及连接数的控制策略。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括同一网络区域的统一出口设计、对未授权外联行为的监控设计、对不同等保级别系统的安全区域的划分、安全区域间访问控制策略设计等。

4.1.2 入侵防范设计

此处描述系统针对端口扫描、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的防范措施，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括对攻击行为的监视。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括对攻击行为的记录和报警、 对恶意代码的检测和清除、 对恶意代码库的更新和系统更新。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括对攻击行为的记录和报警、 对恶意代码的检测和清除、 对恶意代码库的更新和系统更新。。

4.1.3 结构安全设计

此处描述系统针对网络结构的防护技术，包括：使用交换网络、网络结构划分、地址绑定、 VPN，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括根据信息重要性的不同划分不同的子网或网段。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括地址的绑定， VPN 的配置等。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括对网络区域内所有设备的自动识别与定位、地址的绑定。

4.2 主机安全设计

4.2.1 操作系统

4.2.1.1 安全基线配置

此处描述系统依据安全需求分析及公司基线要求所采用身份鉴别、访问控制、安全审计、入侵防范及恶意代码防范、资源控制、剩余信息保护策略，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括

身份鉴别方面：对操作系统用户身份的标识和唯一性、静态口令的组成要求策略、登录失败处理、管理用户鉴别信息传输安全性；

访问控制方面： 安全控制策略制定、 权限分离原则、 多余和过期账号的处理、默认账号限制；

安全审计方面： 审计覆盖范围、 审计内容、 审计记录的保护及保存时间设定；具体采用的操作审计产品型号及数量，部署位置，部署目的，主要的配置策略。
具体采用的监控审计产品型号及数量，部署位置，部署目的，主要的配置策略。

入侵防范及恶意代码防范方面：操作系统的最小安装原则、恶意代码软件的安装、更新以及统一管理；

资源控制方面：终端接入方式、网络地址范围定义、操作超时处理、单个用户对资源的最大及最小使用限度控制。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技

术设计，包括

身份鉴别方面： 静态口令的更换期限设定、 必须采用两种或两种以上组合的鉴别技术、 主机对相连服务器及终端设备的身份标识和鉴别、 使用加密技术防止鉴别信息传输中被窃听、重要信息资源设置敏感标记并根据安全策略进行访问；

访问控制方面：用户最小权限原则；

安全审计方面：审计数据分析及报表实现、审计进程的保护避免受到中断；

剩余信息保护方面： 对鉴别信息、 系统文件、 目录和数据库记录等资源所在的存储空间，被释放或再分配给其他用户时，得到完全清除；

入侵防范及恶意代码防范方面：入侵行为的检测、记录和报警，对重要程序的完整性检测以及破坏后的恢复措施，主机恶意代码库必须独立网络恶意代码库；

资源控制方面：对重要服务的监视、对系统服务服务水平最小值进行设置、检测和报警。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外， 需要符合的商密增强要求的设计， 包括：

身份鉴别：口令策略必须通过技术手段加以保障，系统用户必须由单位内部人员进行统一管理和使用、必须采用两种或两种以上组合的鉴别技术；

访问控制：账号开设的审批程序及留档、账号权限及用户角色的对应、账号的审核机制；

入侵防范及恶意代码防范方面：软件白名单及黑名单的管理、禁止通过互联网在线安装及升级软件；

4.2.2 数据库

4.2.2.1 安全基线配置

此处描述系统依据安全需求分析及公司基线要求所采用身份鉴别、访问控

制、入侵防范、资源控制、剩余信息保护策略，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括

身份鉴别方面：对数据库用户身份的标识和唯一性、静态口令的组成要求策略、登录失败处理、管理用户鉴别信息传输安全性；

访问控制方面： 安全控制策略制定、 权限分离原则、 多余和过期账号的处理、默认账号限制；

安全审计方面： 审计覆盖范围、 审计内容、 审计记录的保护及保存时间设定；

入侵防范及恶意代码防范方面：操作系统的最小安装原则、恶意代码软件的安装、更新以及统一管理；

资源控制方面：终端接入方式、网络地址范围定义、操作超时处理、单个用户对资源的最大及最小使用限度控制。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括

身份鉴别方面： 静态口令的更换期限设定、 必须采用两种或两种以上组合的鉴别技术、 主机对相连服务器及终端设备的身份标识和鉴别、 使用加密技术防止鉴别信息传输中被窃听，重要信息资源设置敏感标记并根据安全策略进行访问；

访问控制方面：用户最小权限原则；

安全审计方面： 审计数据的分析及报表的形成、 审计进程的保护避免受到中断；具体采用的操作审计产品型号及数量，部署位置，部署目的，主要的配置策略。具体采用的数据库审计产品型号及数量，部署位置，部署目的，主要的配置策略。

剩余信息保护方面： 对鉴别信息、 系统文件、 目录和数据库记录等资源所在

的存储空间，被释放或再分配给其他用户时，得到完全清除；

入侵防范及恶意代码防范方面：入侵行为的检测、记录和报警，对重要程序的完整性检测以及破坏后的恢复措施，主机恶意代码库必须独立网络恶意代码库；

资源控制方面：对重要服务的监视、对系统服务服务水平最小值进行设置、检测和报警。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外， 需要符合的商密增强要求的设计， 包括：

身份鉴别：口令策略必须通过技术手段加以保障，系统用户必须由单位内部人员进行统一管理和使用、必须采用两种或两种以上组合的鉴别技术；

访问控制：账号开设的审批程序及留档、账号权限及用户角色的对应、账号的审核机制；

入侵防范及恶意代码防范方面：软件白名单及黑名单的管理、禁止通过互联网在线安装及升级软件；

4.2.2.2 数据库 HA （可选）

此处描述实现数据库 HA 具体采用的产品型号及数量， 部署位置，部署目的，主要的配置策略。

4.2.3 中间件

4.2.3.1 安全基线配置

此处描述系统依据安全需求分析及公司基线要求所采用身份鉴别、访问控制、入侵防范、资源控制、剩余信息保护策略，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括

身份鉴别方面：对数据库用户身份的标识和唯一性、静态口令的组成要求策略、登录失败处理、管理用户鉴别信息传输安全性；

访问控制方面： 安全控制策略制定、 权限分离原则、 多余和过期账号的处理、默认账号限制；

安全审计方面： 审计覆盖范围、 审计内容、 审计记录的保护及保存时间设定；系统具体采用的操作审计产品型号及数量， 部署位置， 部署目的， 主要的配置策略。

入侵防范及恶意代码防范方面：操作系统的最小安装原则、恶意代码软件的安装、更新以及统一管理；

资源控制方面：终端接入方式、网络地址范围定义、操作超时处理、单个用户对资源的最大及最小使用限度控制。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括

身份鉴别方面： 静态口令的更换期限设定、 必须采用两种或两种以上组合的鉴别技术、 主机对相连服务器及终端设备的身份标识和鉴别、 使用加密技术防止鉴别信息传输中被窃听，重要信息资源设置敏感标记并根据安全策略进行访问；

访问控制方面：用户最小权限原则；

安全审计方面： 审计数据的分析及报表的形成、 审计进程的保护避免受到中断；

剩余信息保护方面： 对鉴别信息、 系统文件、 目录和数据库记录等资源所在的存储空间，被释放或再分配给其他用户时，得到完全清除；

入侵防范及恶意代码防范方面：入侵行为的检测、记录和报警，对重要程序的完整性检测以及破坏后的恢复措施，主机恶意代码库必须独立网络恶意代码

库；

资源控制方面：对重要服务的监视、对系统服务服务水平最小值进行设置、检测和报警。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括：

身份鉴别：口令策略必须通过技术手段加以保障，系统用户必须由单位内部人员进行统一管理和使用、必须采用两种或两种以上组合的鉴别技术；

访问控制：账号开设的审批程序及留档、账号权限及用户角色的对应、账号的审核机制；

入侵防范及恶意代码防范方面：软件白名单及黑名单的管理、禁止通过互联网在线安装及升级软件；

4.2.3.2 中间件 HA （可选）

此处描述实现中间 HA 具体采用的产品型号及数量，部署位置，部署目的，主要的配置策略。

4.3 应用安全设计

4.3.1 身份鉴别防护设计

此处描述系统针对暴力猜解攻击的防护技术和产品，包括：身份认证手段、密码强度、密码有效期、图片验证码、认证失败处理方式，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括使用专用登录控制功能、提供用户身份标识唯一性和复杂度检查功能、登录失败处理功能、用户鉴别信息复杂度检查策略可配置。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，　根据等保三级要求还需采用的技术设计，包括对同一用户应采用两种或两种以上组合的鉴别技术实现用户身份鉴别，应用软件对用户在线超时时间的设定以及处理，　用户初始密码的强制修改设计，密码强度、密码有效期策略设计。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括对用户账号的定期清查，　密码强度及密码有效期策略设计及实现技术手段，　应由单位内部人员进行用户的统一管理和使用。

4.3.2　访问控制防护设计

此处描述系统针对信息泄漏的防护技术，包括：用户分类管理、重要用户安全管理、角色定义、权限划分、授权粒度，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括访问控制功能设计，访问控制策略设计，访问控制范围，账号最小权限原则，默认账号的访问权限限制，关键用户及权限的对应关系表设计。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，　根据等保三级要求还需采用的技术设计，包括对重要信息资源设置敏感标记的功能及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。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括账号开设的审批流程、审批主管部门以及留档设计

4.3.3 自身安全防护设计

4.3.3.1 注入攻击防护设计

此处描述系统针对注入攻击的防护技术和产品，包括：程序开发的输入检测、应用防火墙。

4.3.3.2 漏洞利用防护设计

此处描述系统针对缓冲区漏洞、 unicode二次编码等漏洞的防护技术和产品，包括：程序开发的输入数据、应用防火墙。

4.3.3.3 防篡改设计

此处描述系统针对防篡改的技术和产品，包括：网页防篡改。

4.3.4 应用审计设计

阐述本系统的审计对象、范围（操作、事件） 、格式、报表要求，审计日志的保存期， 防删改的要求， 根据系统等保级别的不同采用以下不同的设计， 商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括审计功能应覆盖每个用户，审计记录的不可删除、 修改和覆盖，审计记录的内容应包含事件日期、时间、发起者信息、 类型、描述和结果， 审计记录保存时间设定并不少于一个月。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括审计进程的独立性及不可中断， 审计记录保存时间设定并不少于半年，审计记录数据地统计、查询、分析及生成审计报表的功能设计，每次登录时应显示上次成功登录的记录。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括集中审计数据存储、传输、外放使用、打印等行为的审计、外放内容审计。

4.3.5 通信完整性防护设计

此处描述系统针对通信完整性的防护技术，包括：使用消息摘要、SSL，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括保证通信过程中数据的完整性所采用的校验码技术。

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，根据等保三级要求还需采用的技术设计，包括保证通信过程中关键数据完整性所应采用的密码技术。

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计。

4.3.6 通信保密性防护设计

此处描述系统针对嗅探的防护技术，包括：使用SSL，数据加密，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括会话初始化验证时应用系统采用的密码技术，敏感信息通信过程中的加密设计；

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，根据等保三级要求还需采用的技术设计，包括对于通过互联网对外提供服务的系统，在通信过程中的整个报文或

会话过程中使用的专用通信协议或加密方式设计；

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计。

4.3.7 防抵赖设计

此处描述系统针对防抵赖的技术和产品，包括：日志，数字签名，根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保三级要求

此处描述系统根据等保三级要求采用的技术设计，　包括实现为数据原发者及接收者提供数据原发及接收证据功能的技术设计，包括日志、数字签名等。

2) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括实现为数据原发者及接收者提供数据原发及接收证据功能的技术设计，包括日志、数字签名等。

4.3.8 系统交互安全设计

4.3.8.1 本系统涉及的相关系统说明

此处描述所有和本系统互联的系统介绍，传输的数据类型，采用的传输方式

4.3.8.2 系统交互安全性设计

此处描述系统间交互采用的方式（接口还是非接口）　，采用的安全设计，包括：设备部署、传输协议、数据加密、边界访问控制、授权、审计

4.3.8.3 系统安全监控和检测设计

此处描述系统间交互采用的安全监控和检测设计，包括：协议分析和流量统计、操作审计、数据库审计、集中审计监控、边界访问控制、授权、审计

4.4 数据及备份安全设计

4.4.1 数据的保密性设计

此处描述数据的保密性设计，包括：访问限制、身份鉴别、数据采集的保密性、数据传输的保密性、数据使用的保密性、数据存储的保密性、数据删除的保密性。根据系统等保级别的不同采用以下不同的设计， 商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括实现鉴别信息存储的保密性所采用的加密或其他保护措施设计；

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括实现系统管理数据、鉴别信息和重要业务数据采集、传输、使用和存储过程的保密性所采用加密或其他有效措施设计；

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括数据的分级，密级标识及防护策略设计，数据存储类型分类及防护策略的设计，防止数据存储介质丢失或信息非法泄露的技术设计， 数据传输的加密设计、 外带数据的加密设计， 导出数据的审批授权设计， 无线网络传输时采用的动态加密技术，。

4.4.2 数据的完整性设计

此处描述数据的完整性设计、 包括：数据采集的完整性、 数据传输的完整性、数据处理的完整性、 数据使用的完整性、 数据导出的完整性， 根据系统等保级别的不同采用以下不同的设计，商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括实现鉴别信息和重要业务数据在传输过程中完整性受到破坏时所采用的检测技术设计；

2) 等保三级要求

此处描述系统除了等保二级要求的技术外，　根据等保三级要求还需采用的技术设计，包括实现系统管理数据、鉴别信息和重要业务数据在采集、传输、使用和存储过程中完整性受到破坏时所采用的检测技术设计，　以及检测到完整性错误时采取必要的恢复措施设计；

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括实现系统管理数据、 鉴别信息和重要业务数据在采集、 传输、使用和存储过程中完整性受到破坏时所采用的检测技术设计，　以及检测到完整性错误时采取必要的恢复措施设计。

4.4.3　数据的可用性设计

此处描述数据的可用性设计，包括：数据采集的可用性、数据传输的可用性、数据处理的可用性、数据使用的可用性、数据导出的可用性。

1) 商密增强要求（补充）

此处描述系统除了以上设计外，需要符合的商密增强要求的设计，包括数据传输黑白名单的设计，数据使用用户与使用权限的关联设计。

4.4.4　数据的不可否认性设计

此处描述数据的不可否认性设计，包括：审计、数据采集的不可否认性、数据传输的不可否认性、数据使用的不可否认性、数据删除的不可否认性。

1) 商密增强要求（补充）

此处描述系统除了以上设计外，需要符合的商密增强要求的设计，包括数字水印的设计，打印、传真、刻录、拷贝、删除等行为审计和控制设计，核心商密

数据处理流程的审批以及审计设计， 专用终端的身份认证、 控制与管理设计， 专用终端的桌面安全设计。

4.4.5 备份和恢复设计

4.4.5.1 系统存储设计

此处描述系统针对存储介质的要求，数据不同分类存储

4.4.5.2 系统备份和恢复设计

4.4.5.2.1 系统备份

4.4.5.2.1.1 备份数据类型

此处描述系统备份的数据类型，包括：系统文件、应用软件、业务数据、日志信息、历史数据

4.4.5.2.1.2 备份方式

此处描述各种数据类型的备份方式，包括：硬盘文件、磁带

4.4.5.2.1.3 备份策略

此处分别针对联机事务处理系统、信息管理系统、决策支持分析系统描述备份的具体策略。 根据系统等保级别的不同采用以下不同的设计， 商密增强要求作为补充要求：

1) 等保二级要求

此处描述系统根据等保二级要求所采用的技术设计，包括对重要信息进行备份的策略设计；数据处理系统的冗余设计；

2) 等保三级要求

此处描述系统除了等保二级要求的技术外， 根据等保三级要求还需采用的技术设计，包括实时备份和异步备份、 增量备份与完全备份的设计， 异地数据备份

的要求及设计， 备份技术的可行性验证测试设计， 异地数据备份中心的可用性设计；

3) 商密增强要求（补充）

此处描述系统除了符合等保要求外，需要符合的商密增强要求的设计，包括实时备份和异步备份、 完全备份的设计， 异地数据备份的要求及设计， 异地数据备份中心的可用性设计。