**XXX单位**

**应用安全管理规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479432564)

[2 适用范围 1](#_Toc479432565)

[3 应用管理 1](#_Toc479432566)

[3.1 身份鉴别 1](#_Toc479432567)

[3.2 访问控制 1](#_Toc479432568)

[3.3 日志审计 2](#_Toc479432569)

[3.4 安全传输 2](#_Toc479432570)

[3.5 资源利用 2](#_Toc479432571)

[3.6 安全管理 2](#_Toc479432572)

[4 附则 3](#_Toc479432573)

# 目的

应用系统是业务管理和数据输入输出平台，应用安全即保障应用程序使用过程和结果安全，就是针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃，通过其他安全工具或策略来消除隐患。

本文档规定了XXX单位应用安全管理要求及规范。

# 适用范围

本文档适用于XXX单位信息系统中应用系统。

# 应用管理

## 身份鉴别

1）登录应用系统需要通过用户名和密码鉴别认证。

2）应对应用系统中的用户进行标识，用户标识应遵守唯一性原则，并将用户标识与审计相关联。

3）应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

4）应在登录过程中确保鉴别信息是保密的，不易伪造的。

## 访问控制

1）应对应用系统的访问设定访问控制规则，减少非授权访问。

2）应用系统应按照最小权限原则对不同用户进行授权，保证各用户权限最小化。

3）应用系统的安装目录和文件的访问权限应进行最小化设置，防止未授权用户访问相关资源。

4）应用系统应启用登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施。

## 日志审计

1）应为应用系统建立独立的日志审计系统，定义与应用安全相关的日志审计事件记录。

2）能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏。保护审计数据，严格限制未经授权的用户访问。

## 安全传输

1）对应用系统进行管理时，应采取一定的安全机制，防止鉴别信息和管理数据在网络传输过程中被窃听。

2）应用系统与第三方系统进行数据交互时，应采用加密措施保护数据信息传输安全。

## 资源利用

1）应对应用系统的最大并发会话连接数进行限制，防止受到拒绝服务攻击。

2）应对应用系统内单个帐户的多重并发会话进行限制，并对会话超时进行重鉴别控制。

3）应对应用系统资源进行监视，并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。

## 安全管理

1）设置应用系统审计管理员、系统管理员角色、系统安全管理员角色，并且实现不同管理用户的权限分离，仅授予管理用户所需的最小权限，同时系统审计管理员角色与系统管理员角色、系统安全管理员角色不能是同一人担任。

2）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。

3）应用系统提供自动保护功能（如守护进程重启故障中断的服务进程等），确保能够自动保护当前所有状态，保证系统能够进行恢复。

4）应用系统应定期进行系统版本更新和补丁更新。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。