**XXX单位**

**主机安全管理规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479441441)

[2 适用范围 1](#_Toc479441442)

[3 办公终端管理 1](#_Toc479441443)

[3.1 管理要求 1](#_Toc479441444)

[3.2 设备安全 1](#_Toc479441445)

[4 主机系统管理 2](#_Toc479441446)

[4.1 设备安全 2](#_Toc479441447)

[4.2 系统管理 2](#_Toc479441448)

[4.3 安全管理 3](#_Toc479441449)

[4.4 备份恢复 3](#_Toc479441450)

[5 附则 4](#_Toc479441451)

# 目的

主机系统是各类业务系统数据和信息的主要载体，病毒、攻击入侵等安全威胁很容易通过访问主机系统的终端渗透到后台各种业务应用和服务主机中，从而对业务平台系统的整体安全带来危害。

本文档规定了XXX单位主机系统安全管理要求规范，指导业务平台主机的安全配置和维护，从而提高业务平台各系统的总体安全水平。

# 适用范围

本文档适用于适用于XXX单位主机系统。

# 办公终端管理

## 管理要求

按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”原则，明确主管单位、运维单位和使用单位的安全责任。

采用集中管理措施，统一部署防病毒系统、统一部署终端安全管控系统以及统一系统升级。

应针对办公终端物理安全、系统软件、应用软件、安全审计、安全防护、外围设备安全各个层面存在的脆弱性进行综合考虑。

办公终端应提供相应的USB接口供移动存储介质，并对移动介质接入进行管控。

对没有必要使用光驱的计算机，取消安装光驱驱动器，也可以通过管理制度约束控制。

## 设备安全

依据《物理安全管理规范》中办公设备安全策略要求。

# 主机系统管理

## 设备安全

依据《物理安全策略》中机房设备安全策略要求。

务终端服务器应用针对在不同的场合时具备防火、防盗、防尘、防淋、防震、防暴等要求，保证人身安全。

## 系统管理

1）应采购正版或合法软件以及相关服务。

2）主机系统应统一命名，名称应易于识别与管理。

3）应对登录主机系统的用户进行身份标识和鉴别，且用户的标识应唯一，根据不同的使用人员分配不同的账号或账号组，删除、锁定或修改系统默认的账号及口令，删除或锁定与设备运行和维护无关的账号。

4）应根据不同的用户或角色分配不同的账号和账号组，避免不同角色之间共享账号。

5）密码应符合口令复杂度要求、最长留存期要求以及连续认证失败次数账户锁定要求。

6）应对登录主机系统的用户进行角色划分，至少包含管理员角色、安全员角色和审计员角色，根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

7）应根据主机终端的日常业务需求，建立终端计算机软件清单，安装业务开展所必需的计算机软件。可包括输入法软件、文档编辑软件、文件压缩软件、网页浏览软件、邮件客户端、文件阅读器、图片查看器、媒体播放、安全防护软件以及打印机等办公设备驱动软件等。

8）应依照主机终端软件选用列表，采购正版或合法软件以及相关服务，建立软件资产清单。

## 安全管理

1）应启用日志审计功能，不仅包括对用户登录、用户操作进行记录，也要包括系统事件，安全事件等，日志应妥善保存、定期审计分析和备份，并确保日志记录的完整性。

2）应对主机系统资源使用情况进行监控，监控内容包括CPU使用率、硬盘使用率、内存使用情况等信息。

3）应启用防火墙功能并安装统一的防病毒产品，设置统一的防毒策略，实时防治病毒，防病毒系统应自动保持防病毒代码的更新，或者通过运维操作员进行手动更新。

4）在对主机操作系统的补丁进行更新前，应对补丁与现有业务系统的兼容性进行测试，确认后与系统提供厂商配合进行相应的修复。

5）应对操作系统的漏洞发展情况进行跟踪，形成详细的安全更新状态报表。安装补丁软件包则以必要为原则，非必需的就不装。

6）主机系统远程管理过程中，应采用安全可靠的加密协议对通信过程中的整个报文或会话过程进行加密。

7）主机系统应对连接超时进行限制，当用户登录设备后，一段时间未进行操作后，就将自动中断此用户的连接。

8）业务终端服务器在安装时选择必要组件，禁止安装与业务无关的组件，关闭不必要的服务，关闭自动播放功能。

## 备份恢复

备份应该采用合适的技术手段，实现对主机系统进行备份（数据库及应用数据备份内容不在本规范的定义范围之内），主要的技术要求如下：

1）应对主机系统进行统一的容灾备份，根据业务系统的重要程度，对主机系统进全备份或者关键配置信息备份。

2）应具有对备份操作进行记录并可查询。

3）应考虑定期进行恢复性测试，以确保备份数据的可恢复性。

4）备份内容应定期转储存放到外部介质上（如磁带、光盘、服务器等），且上述外部介质应存放在与业务系统不同的位置。

# 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。