**XXX单位**

**系统安全管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479446856)

[2 适用范围 1](#_Toc479446857)

[3 管理内容和办法 1](#_Toc479446858)

[3.1 操作系统安全管理 1](#_Toc479446859)

[3.2 数据库系统安全管理 2](#_Toc479446860)

[3.3 系统上线前的安全检查 3](#_Toc479446861)

[3.4 系统补丁安全管理 3](#_Toc479446862)

[3.5 漏洞发现与安全通告要求 3](#_Toc479446863)

[3.6 测试与安装前准备要求 4](#_Toc479446864)

[3.7 信息安全等级保护 5](#_Toc479446865)

[4 附则 5](#_Toc479446866)

# 目的

为规范系统的管理和运行维护，提高服务质量，保障信息系统安全、稳定运行，特制定本制度。

# 适用范围

本制度适用于XXX单位系统安全管理和运行工作。

# 管理内容和办法

## 操作系统安全管理

1）身份鉴别

* 应提供用户身份标识唯一和鉴别信息复杂度检查功能，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。
* 应更改默认的系统管理员帐号和口令，管理员帐号应采用实名制。
* 应启用控制台锁定功能，屏幕保护程序在恢复控制台显示之前，应要求用户名和口令认证。
* 应对操作系统文件、目录的访问权限进行控制。
* 应提供登录失败处理功能，并且采取结束会话、限制非法登录次数和自动退出等措施。
* 禁止从互联网远程登录服务器，内部网络登录服务器应该限制其登录源IP或MAC地址以及用户捆绑。

2）只启用系统需要发挥作用的服务，并开启其端口，限制或关闭不需要的服务或端口。

3）关键业务信息系统要定期进行漏洞检查，并确定是否需要进行安全加固，必须定期更新操作系统防病毒软件特征库，并做好记录。

4） Windows操作系统应进行注册表安全检查（如：禁止在任何驱动器上自动运行任何程序，用星号掩藏任何口令输入等）。

5）应开启访问、认证、授权的安全审计策略；启用日志审计功能。

6）时钟同步设置，XX单位内所有等保二、三级的信息系统及相关的重要网络设备的时钟应使用已设的精确时间源进行同步。

## 数据库系统安全管理

1）数据库环境安全

* 数据库服务器应当置于单独的服务器区域，任何对这些数据库服务器的物理访问均应受到控制。
* 数据库服务器所在的服务器区域边界应部署防火墙或其它逻辑隔离设施。
* 数据库系统的宿主操作系统除提供数据库服务外，不得提供其它网络服务，如：WWW、FTP、DNS等。
* 应在宿主操作系统中设置本地数据库专用帐号，并赋予该账户除运行各种数据库服务外的最低权限。
* 应对数据库系统安装目录及相应文件访问权限进行控制，如：禁止除专用账户外的其它账户修改、删除、创建子目录或文件。

2）数据库系统安装、启动与更新

* 应注意生产数据库系统应与开发数据库系统物理分离，确保没有安装未使用的数据库系统组件或模块。
* 仅开启必须的数据库系统服务。
* 经过测试，在确保数据库系统稳定运行的前提下，安装最新补丁。
* 数据库系统管理员应定期检查数据库系统完整性。

3）数据库对象安全

* 应更改默认数据系统管理员帐号和口令。
* 应对数据文件访问权限进行控制，如：禁止除专用账户外的其它账户访问、修改、删除数据文件。
* 删除不需要的示例数据库，在允许存在的示例数据库中严格控制数据库账户的权限。
* 具体数据库权限管理要求参见5.3.2 章节部分。
* 应注意删除或禁用不需要的数据库存储过程。
* 对于数据库中的敏感字段，如：口令等，应加密保存。
* 应启用数据库日志审计功能。
* 定期对数据库配置参数进行备份，数据库数据备份、恢复管理。

## 系统上线前的安全检查

系统在上线前应进行安全检查，检查至少包括以下内容：

1）认证口令存储是否加密。

2）是否具有登录认证失败后的处理方式。

3）是否对不同用户的访问权限进行严格的访问控制，特定权限的用户只能看到和使用特定的界面及相应的功能。

4）系统是否存在安全漏洞。

5）日志记录内容是否满足审计要求，日志保存时间是否在两个月以上。

6）是否设置了时钟同步。

## 系统补丁安全管理

1）系统软件管理范围包括服务器上运行的操作系统和应用软件，网络及安全设备上运行的操作系统等。

2）安全补丁根据其对应漏洞的严重程度分为三个级别：紧急补丁、重要补丁和一般补丁；紧急补丁必须在15天内完成安装，重要补丁必须在一个月内完成安装，一般补丁要求六个月内完成安装。特殊情况另外处理。

3）本局范围内同类型设备应保持装载软件版本，补丁的一致性。

4）做好应用软件版本及安全补丁的归档管理，以备回滚或系统重装时使用，并建立相关的文档资料收集和整理工作。

## 漏洞发现与安全通告要求

1）信息中心及时收集系统软件存在的漏洞，及时发布预警工作。

2）应定期进行漏洞扫描，对发现的安全漏洞进行及时的修补。

3）安全管理员通过邮件形式统一向各级系统管理员、系统维护人员通告安全补丁信息。

4）安全管理员负责对安全补丁进行完整性校验，确保获取的安全补丁软件未被修改和可用。

## 测试与安装前准备要求

1）补丁安装之前应经过严格的测试，不应未经测试直接在现有系统上安装补丁。

2）应用软件版本升级测试尽可能由系统集成商负责实施，业务系统管理员负责协调，应对补丁的现场测试限定测试时间，测试完成后需要编写详细的测试报告，给出明确的测试结论。补丁测试的内容包括补丁安装测试、补丁功能性测试、补丁兼容性测试和补丁回退测试。

3）服务器的补丁安装，尽可能在其他备用设备上进行测试。

4）安全测试主要测试补丁安装过程是否正确无误，补丁安装后系统是否正常启动；

5）补丁功能性测试主要测试补丁是否对安全漏洞进行了修补；

6）补丁兼容性测试主要测试补丁加载后是否对应用系统带来影响，业务是否可以正常运行；

7）补丁回退测试主要包括补丁卸载测试、系统还原测试。

8）各业务系统管理员应把补丁的测试报告，提交给安全管理员，并提交信息中心负责人进行审核，审核通过后方可进行补丁安装。

9）为确保系统集成商及时配合补丁的测试和安装工作，需要通过合同的方式，明确集成商的安全补丁测试和安装责任，约束条款至少应包括：实验室测试环境的搭建，在规定时间内完成补丁测试，补丁的安装，补丁安装失败时的测试与分析，补丁与应用冲突时的系统改造和升级工作。

10）补丁安装的触发条件是安全检查，巡检发现，功能需求，主动漏洞扫描等。补丁应经测试并得到信息安全工作组审核通过，由负责业务组在ITSM服务系统上发起事件申请，并提交实施方案，测试工作具体由涉及相关业务组测试或协助测试。

## 信息安全等级保护

1）系统定级及审批

* XX单位本部、直属中心机构及其直属单位应依据国家颁布的《信息安全等级保护管理办法》对信息系统安全进行定级。
* 安全保护等级为第二级及以上的系统，应当在系统投入运行后30日内办理备案手续。
* 信息安全等级保护应遵循“自主定级、自主保护”原则，各直属单位三级及以上信息系统，报XX单位审核批准后，到所在地的公安机关办理备案手续；XX单位本部三级及以上信息系统向广东省公安厅备案。

2）信息系统等级测评

* 等级测评工作应由具有国家相关技术资质和安全资质的测评单位承担。
* 对于新建、改建、扩建的二级及以上信息系统，应该依照相关规定，经测评机构测评合格方可投入使用，安全测评和风险评估要形成相关文档，作为项目验收的重要内容。
* 等级为三级的信息系统应当每年至少进行一次等级测评，等级为四级的信息系统应当每半年至少进行一次等级测评。

3）信息系统等级保护

* 应按信息系统安全等级保护的相关要求，落实各信息系统的防护措施。

# 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。