计算机网络信息安全管理实施细则

 第一条 目的

为了维护计算机信息系统的安全，促进计算机的应用和发展，保障信息化建设的顺利进行，制定本细则。

 第二条 适用范围

本细则为数据库管理、网络管理和系统管理提供了安全管理的指导规范。

 第三条 方法和要求

第一条 账户管理

账户设立与管理，必须遵循以下原则：

1．以最少授权为原则，严格划分不同用户的访问权限，避免越权访问或交叉授权；

2．以“不肯定即为否定”原则设计访问权限的管理方案；

3．数据库管理人员和网络管理人员、系统管理人员相互制约；

4．考虑针对内部用户和外部用户的不同的安全策略；

5．考虑权限管理配置的灵活性和可扩展性。

第二条 口令管理

1．所有账户必须都设有口令；

2．口令应当至少有8个字符长，使用大小写字母，数字混编，且建议口令中要有一些非字母（如标点符号等）；

3．设定口令的存活期为一个月，禁止自始自终一成不变的用户口令；

4．不准使用用户名（账号）作为口令；

5．不准使用用户名（账号）的变换形式作为口令；

6．不准使用自己或者亲友的生日作为口令；

7．不准使用常用的英文单词作为口令。

第三条 病毒防治

1．建立病毒服务器，及时查杀服务器、客户端病毒；

2．定期对网络版病毒防治软件进行安全评估，并及时对其升级；

3．限制共享目录及读写权限的使用；

4．限制网上软件的下载和禁止盗版软件；

5．对外来的软盘必须先查毒后使用；

6．将服务器上某些可执行文件的写属性设为禁止。

第四条 网络管理

1．合理划分网段，减少无用的广播包括对网络攻击的风险；

2．使用网络日志，对网络进行适当监控；

3．通过定义虚拟子网隔断非法访问；

4．通过IP地址与网卡MAC地址捆绑的方法防止IP盗用。

第五条 系统管理

1．在各种操作系统使用最新的补丁；

2．定期对服务器尤其是关键的服务器进行安全评估，发现其中的安全漏洞， 根据专家建议进行修补；

3．禁止从软盘、光驱引导（随机盘除外）；

4．设置开机口令；

5．设置屏幕保护口令；

6．在Windows server中只使用NTFS或更高级格式；

7．尽量少将应用程序设置成自动登录；

8．删除不用的账号；

9．采用“悲观法”进行安全设置。

第六条 数据库管理

1．在各种数据库使用最新的补丁；

2．定期对数据库进行安全评估，发现其中的安全漏洞，根据专家建设进行 修补；

3．删除不用的账号。

第七条 网络设备管理

1．在路由器和交换机上定义访问属性，只允许经过认证的；

2．正常数据访问请求通过，非法的访问请求被拒绝并记录日志。

 湖南交通工程学院

 信息中心汇编

 2022年1月22日