**XXX单位**

**账户权限、口令管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479445450)

[2 适用范围 1](#_Toc479445451)

[3 账号和权限管理 1](#_Toc479445452)

[4 口令管理 2](#_Toc479445453)

[5 附则 3](#_Toc479445454)

# 目的

本规范规定了XXX单位信息系统账号权限、口令管理要求。

# 适用范围

本规范适用于XXX单位操作系统、数据库、网络设备和业务应用。

# 账号和权限管理

1）员工录用时，人事部门或调入部门必须及时书面通知信息技术部门添加相关的帐号、口令及权限等。

2）员工在岗位变动时，人事部门或调入部门必须及时书面通知信息技术部门修改和删除相关的帐号、口令及权限等。

3）员工调离时必须由人事部门书面通知信息技术部门删除相关的帐号、口令及权限等。

4）操作人员访问权限的授予、变更和注销严格按照相关流程进行审批，经全部审批完毕后方给予相应权限。

5）将系统管理员权限和数据库管理员权限分开授予，禁止同一人掌管操作系统口令和数据库管理系统口令。授予用户的身份应是唯一的，即一个用户账户唯一地对应一个用户，不允许多人共享一个账户。

6）系统管理员负责用户账号、权限和密码的集中管理，至少每半年审核一次。

7）各级信息技术部门系统管理员应该制定用户权限表，定期对用户的访问权限进行检查。

8）对任何用户的登录应进行身份鉴别。身份鉴别的方法应根据用户所处环境的风险确定。

9）在新系统实施阶段，对于服务提供商需要访问系统，应当采取以下措施：

10）每个应用系统项目组将自己所需要的权限列表，交给信息技术处登记注册。以后有变更的，及时通知信息技术处；

11）原则上不给服务提供商系统管理员的权限；

12）对于无法操作某些功能的情况下，经申请同意可以赋予服务提供商系统管理员的权限，一个项目小组只能有一个系统管理员的帐号，该用户不得将系统管理员的权限赋予他人；

13）实施结束后，系统管理员应当及时删除有关用户账号权限。

14）未经允许，系统管理员不得私自在系统内添加、删除用户，不得随意更改用户权限，防止非授权用户对数据的使用和修改等。

15）严格按岗位职责设置岗位操作权限，应定期检查操作员的权限，发现岗位操作权限不合理时应立即更正。

16）严格控制数据的备份、恢复、转出、转入权限。严禁未经授权将业务数据等拷贝出系统，转给无关的人员或单位；严禁未经授权进行数据恢复或转入操作。

# 口令管理

1）当系统允许安全管理员分发给一个新用户初始口令时，这个初始口令必须只在第一次登录时有效，登录后必须强制用户选择新的口令。本规定同样适用于管理员为丢失口令的用户分配新口令时的情形。

2）用户遗忘口令时，必须在对该用户进行适当的身份识别后才能向其提供临时口令。

3）在向用户提供临时口令时必须确保口令安全。应避免使用第三方或无保护的（明文）电子邮件。用户应对收到的口令予以确认。

4）安装软件后更改默认的供应商口令。

5）用户禁止在web浏览器或电子邮件客户端保存固定口令。

6）口令不得以可读的形式存储在批处理文件、自动登录脚本、软件宏定义、终端功能键或没有访问控制措施的计算机中。

7）凡是涉及主机、网络、数据库的用户口令（包括初始口令），必须实行专人负责、专门管理。应对操作系统和数据库系统特权用户的权限分离。

8）严密保管主机和数据库超级用户的口令。其口令设置，必须具有较强的保密性，严禁泄露给任何单位和个人，并且必须至少每月更换一次。

9）所有系统级口令（如root、enable、NT admin、应用管理帐号等）必须至少每个季度更换一次。

10）用户不得使用原先已经使用过或类似原先使用过的口令。如果系统支持口令选择认可机制，系统必须防止用户选择已用过的口令作为新的口令。

11）所有终端用户口令（如email、web、桌面系统等）强制每三个月改变一次。

12）禁止把口令告诉他人，例如：不在电话上透露口令、不在email或其他电子通信方式中透露口令、不在其他人面前讨论口令、不暗示口令格式、不要把口令写下或存到任何地方，不要把口令未加密就存到文件中或任何计算机系统中。

13）为防止口令猜测攻击，系统必须严格限制允许的错误口令输入次数。在3次错误口令输入后，相关的用户帐号必须进行锁定，直到管理员将锁定解除，或者临时将口令锁定。如果登录会话来自远程拨号或外部网络，必须切断当前会话。

14）如怀疑口令被攻击，报告给信息技术部门并改变所有口令。

15）信息安全部门或授权代表定期或随机运行解密或猜测工具。如口令在扫描中被猜出或解开，要求用户改变口令。

16）PC 或终端在不用或使用者离开时，应使用密钥锁或等效控制措施（如口令访问）防止他人非法使用。

# 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。