**系统数据安全管理制度**

1. **系统安全**

**1.1账户管理：**

1.1.1.管理员密码由指定人员管理

1.1.2.未经授权不得给他人使用

1.1.3.如需使用管理员用户进行操作，必须做好相关记录。

1.1.4.删除系统不必要的用户

**1.2密码策略**：

1.2.1.指定密码复杂性

1.2.2.密码应满足以下要求：

1）密码长度8个字符以上

2）使用以下组合：a-z A-Z 0-9，以及！@#￥%&\*（）-+

3）密码没3个月至少修改一次

**1.3补丁漏洞**：

1.3.1.定期对系统进行检测

1.3.2。安装最新安全的程序。

**1.4账户权限申请：**

1.4.1.工作人员申请账户权限必须经过系统管理员批准后方可开通1.4.2.对用户下发的权限做好详细记录。

1.4.3.人员离职或调职时需交回相关系统账号密码，经系统管理员删除或变更后方能离职或调职。

**1.5系统管理：**

1.5.1.严禁私自在系统上安装来路不明的软件，以免造成病毒感染

1.5.2.有连接服务器权限的人员，用户界面必需设置屏幕密码，以免他人对造成误操作。

1.5.3.修改文件时必须做好实时备份

**1.6远程登陆**：

1.6.1.禁止root远程登陆

1.6.2限制登陆IP

**1.7服务**：

1.7.1.删除并关闭不必要服务

1. **数据库安全**

**2.1. 基础安全设置：**

1）设置root密码

2）移除匿名用户

3）禁止远程root登陆

4）坚持最小权限原则

**2.2. 连接访问安全：**

1）创建用户时需指定IP地址范围或者固定IP

2）规范数据库管理软件，实现管理软件的标准，统一化

3）禁止明文传播数据库账号密码

4）禁止开发工程师通过应用账户登陆生产数据库

**2.3. 账户安全：**

2.3.1.主要时防止泄露，非必要人员不需要知道账户名称，合理使用自己的账户，保护好账户密码

2.3.2用户账户划分原则

1）超级管理员

2）系统应用账户（比如备份，监控，同步）

3）应用业务账户

4）开发人员账户

**2.4. 密码安全：**

2.4.1.密码复杂性：

尽量并且不要使用固定密码，实行每个用户单独密码，长度16位以上，a-z A-Z 0-9，以及！@#￥%&\*（）-+随机组合

2.4.2.密码过期机制：

根据公司的情况设定密码过期时间，定期修改，同时不可使用重复密码。

**2.5. 端口安全**：

修改默认端口

**2.6. 记录安全：**

删除操作系统记录的敏感数据，及时清理移除和禁用操作记录日志