

系统管理员与备份恢复手册

账户、权限、安全运维、审计与应急

版本：V1.0.0

发布日期：2026-08-14

交付状态：正式交付候选版

1. 管理职责

- 维护管理员与普通用户账户，遵循最小权限，不共享个人账号。
- 维护设备、指标、故障字典、制品和评价边界等主数据。
- 执行备份、恢复演练、日志检查、容量检查、升级审批和安全事件处置。
- 保留导入记录、变更依据、测试报告和验收签字，保证过程可追溯。

2. 权限边界

能力	管理员	普通用户
查看设备、数据与分析	允许	允许
录入测试、故障、退化或制品记录	允许	允许
新增/修改/删除设备与主数据	允许	禁止
配置评价参数、指标和字典	允许	禁止
用户与权限管理	允许	禁止
批量清空、恢复与系统级导入	受控执行	禁止

权限在前端控制之外还由后端强制校验。普通用户绕过界面直接调用受限接口时，服务端仍返回403。

3. 账户安全

1. 首次部署后立即修改 admin 密码，并创建实名管理员日常使用；初始账号仅作应急保留。
2. 密码至少 12 位，混合大小写、数字和符号，不与其他系统复用。
3. 员工离岗、岗位调整或账号异常时立即禁用；每季度复核账户与权限。
4. JWT 签名密钥和数据库密码存放在受控 .env 或密码库，不得写入截图、文档和源代码。

4. 数据备份策略

备份类型	建议频率	保留	用途
每日自动全量备份	每日低峰	30 天	误删、故障恢复
升级前备份	每次升级	至少保留至验收后 30 天	版本回退
月度归档	每月	12 个月或按单位制度	审计与长期留存
恢复演练	每季度	保留演练记录	证明备份可恢复

仅生成备份文件不等于备份成功。每次备份必须通过 `pg_restore --list` 校验，并定期在隔离环境实际恢复。

5. 执行备份

- 1. 在交付根目录执行 `sudo ./backup_all.sh`，同时备份两套数据库。
- 2. 确认“运行备份”目录生成两个非空 `.backup` 文件。
- 3. 将备份复制到独立存储，并记录时间、执行人、文件大小和 SHA-256。
- 4. 使用对应系统 `scripts/backup_database.sh` 可单独备份。

6. 执行恢复

恢复会替换目标数据库，必须在维护窗口由管理员执行。先确认系统、数据库名、备份日期和业务批准。

- 1. 停止业务写入，并对当前数据库再做一次备份。
- 2. 运行 `pg_restore --list` 备份文件，确认目录可读。
- 3. 进入对应系统目录，设置 `CONFIRM_RESTORE` 为目标数据库名后执行 `scripts/restore_database.sh` 绝对路径。
- 4. 恢复后运行状态检查，登录系统抽查用户、设备、记录与分析结果。
- 5. 形成恢复记录，包含原因、备份文件哈希、执行人、验证人和结果。

7. Excel 导入治理

阶段	管理员动作	控制目标
模板	从对应业务页面下载模板或使用交付模板	避免工作表和字段错配
预检	查看工作表、行号、列名和错误原因	错误不进入业务表
确认	核对新增、更新、跳过数量后提交	防止重复和误覆盖
留痕	保留源文件校验值、批次、操作者和结果	支持追溯与复核
纠错	修正源 Excel 后重新预检，不直接改数据库	保持数据来源一致

8. 安全巡检清单

- 容器健康状态正常，数据库端口未对外开放。
- 管理员账户无共享、无离岗遗留，普通用户未获得主数据修改权限。
- 最近备份存在、可读取，季度恢复演练未逾期。
- 磁盘、日志和数据库连接数处于合理范围。
- 交付包哈希未变化，依赖漏洞和 SBOM 已纳入版本升级评估。
- HTTPS 证书有效，服务器系统和 Docker 安全更新按单位窗口执行。

9. 事件响应

事件	立即动作	后续动作
疑似账号泄露	禁用账号、轮换密码和签名密钥、保全日志	核查异常操作并通知负责人
错误批量导入	停止后续写入、保留导入批次与源文件	评估回退或按批次纠错

事件	立即动作	后续动作
数据库损坏	停止业务、保全现状、选择最近可用备份	隔离恢复、校验后切换
服务器故障	在备用服务器部署同版本并恢复数据	复盘硬件、备份和 RTO/RPO