Assignment 1

作为工程师的建议

组建 RAID 阵列：防止物理破坏

组建 RAID 阵列可以有效防止物理破坏导致的数据丢失，并提高服务器的读写速度。如果组建 RAID10 阵列，服务器可以在多块硬盘损坏的情况下不丢失数据，且采用热备份的方式，不会影响服务器的正常运行。

备份数据库：防止数据丢失

公司应对数据库保持一定的备份频率，在出现数据丢失的情况下，可以回滚到最近一次备份的状态。为保证数据安全，应将备份的数据存储在不同的地点，且将访问不同备份的权限分配给不同的人，防止单个人员恶意篡改备份的数据。

考虑到公司的规模较小，传统的两地三中心备份方案不适用。但是可以通过购买云服务器的方式实现热备份或者冷备份。

数据审计：防止数据篡改

通过设置 trigger，可以在每次对数据库进行修改时，将修改的内容记录在日志中。如果发现数据库中的数据被恶意篡改，可以通过日志追踪到修改的时间和修改的内容，从而找到破坏数据库的人。

输入检查：防止 SQL 注入攻击

在设计数据库输入时，使用 prepared statement，可以防止 SQL 注入攻击篡改或者删除数据库中的数据。使用 procedure，可以提前对输入的数据进行检查，同样可以防止恶意操作。

身份验证：防止密码泄露导致的恶意操作

对有权修改数据库的用户，应在操作前进行多重身份验证。例如通过离线应用程序随机生成并不断更新验证码（例如 Google Authenticator），可以保证即使高权限人员密码泄露，攻击者也无法进行恶意操作。

成本估计

项目	成本	说明
本地备份/RAID10 阵列	0.29¥/GB	以西部数据 4TB 黑盘为例
数据库云备份（冷备份）	0.12¥/GB/月（储存费用）+0.75¥/GB（备份费用）	以阿里云 DBS 服务为例
数据库云备份（热备份）	可按需购买计算节点及储存空间	以阿里云 PolarDB PostgreSQL 版为例
数据审计	0.29¥/GB	同本地备份/RAID10 阵列
其余	0.00¥	无需额外成本

作为 CTO 的建议

权限管理：防止低权限用户进行恶意操作

在软件层面，应对用户进行权限管理。例如负责前端的工程师不应该拥有修改数据库的权限，而只能通过调用 procedure 的方式修改数据库，如需要修改数据库，则需要向负责后端的工程师提出申请。负责维护数据库的工程师应该拥有最高权限，但是应该对其进行严格的审计。

已经离职的人员的授权应该被删除，以防止公司以外的人利用账号进行恶意操作。

完善数据库规范

公司可以出台数据库规范或遵守已有的数据库规范，对数据库的设计、维护、备份等方面的操作方法提出要求，并规律性地通过审计来检查规范的执行情况。对于违反规范的人员，应该进行相应的处罚。

同时，应该对有权限修改数据库的人员进行普法教育，提高其安全意识。

完善灾备计划

公司应该制定完善的灾备计划。应规律进行应急演练，模拟数据库被破坏的情况，以保证在真正发生灾难时，公司能够快速恢复。

成本估计

项目	成本	说明
权限管理	开发权限管理软件成本	无需额外成本
数据库规范	0.00¥	无需额外成本
灾备计划	0.00¥	无需额外成本