科然信息系统安全策略

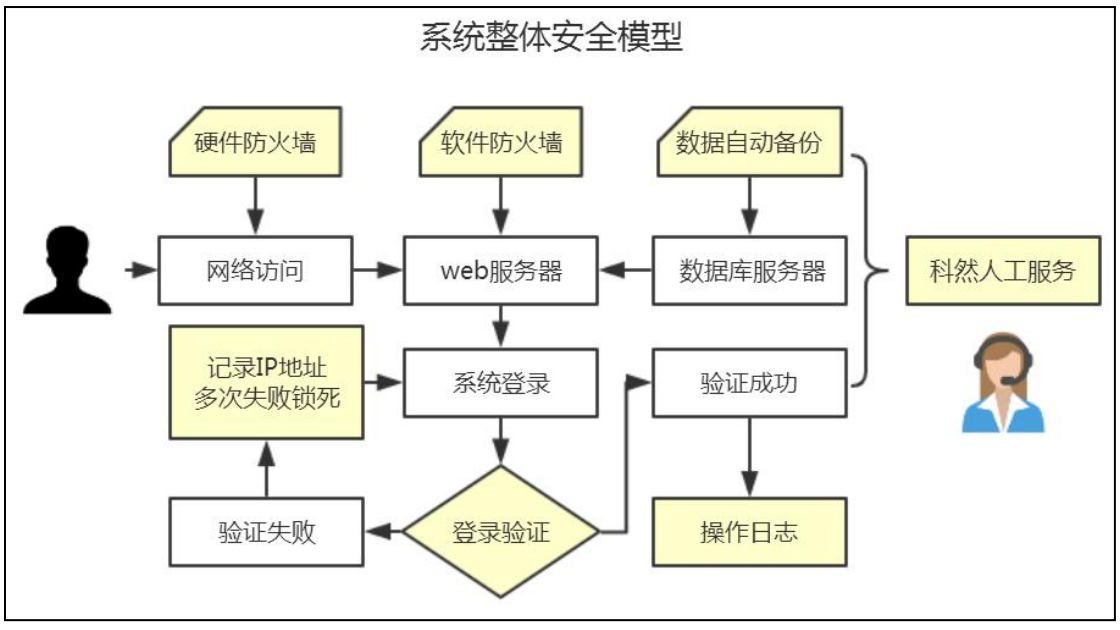
“无安全不运行”。对于暴露在外网的管理系统，安全性无疑是重中之重，系统将所有的登录动作都记录日志，且对登录错误次数过多的 IP 进行封锁，对 SQL 注入等可疑行为进行记录，对数据进行按日备份，从预防到记录到事后补救，各阶段都进行了相应的设计。

系统建议采用双机模式，即：web 服务器和数据库服务器两台服务器的模式，用来实现服务和数据的分离。服务对外，数据隐藏在内部网络中，令系统运行更为安全，另外数据库服务器可根据数据容量分别带有自己的外存磁盘阵列。（如暂时无法到位两台服务器，也可以部署在一台服务器中）

系统安全

系统安全总体设计

系统整体安全模型图：（黄色背景卡片为安全措施节点）



以预防为主的整体安全防护方案

如上图，系统在从网络到 WEB 服务器，到数据库服务器，到软件系统的登录和运行，从预防到灾难发生后的恢复机制，提供了全套的安全解决方案。做到“防患于未然”，如有意外情况也能及时补救。

系统安全分项设计

操作安全性

操作安全性由网络登录验证、数据库登录验证、应用系统使用验证三级组成。网络登录验证由操作系统完成，用于对具有网络资源访问权限用户的验证；数据库登录验证由数据库服务器完成，用于对具有数据库访问权限用户的验证；系统使用验证由应用系统完成，用于对具有应用系统使用权限用户的验证；应用系统将采用三种验证方式相结合的方式验证用户。

数据传输安全性

为保证数据传输的安全性，使得所传输数据不被盗窃、更改，应用系统所采集的重要原始数据可采用网络加密传输、数据库加密传输或应用系统数据加密相结合的技术。

数据存储安全性

重要数据因某种原因需用存储介质进行长期备份存储时，可采用加密算法对数据进行加密，使得非法用户不能理解其含义，当合法用户访问时再将其还原。

全过程日志记录

运用日志，对进入系统的用户的操作进行记录，包括合法用户的操作和非法用户的尝试性登录；可以根据日志进行事后分析，从而找到事故的发生原因、责任者或非法用户。

系统维修时的数据安全性

当系统需要检修或维修时，有可能对系统进行调试，在调试时我们将采用切换到临时运行环境的方法，使系统在调试时与正式存储设备（数据库）隔离，维

修结束正式使用时，再将系统与正式存储设备（数据库）相连接。这样就可以保证系统在维修时已有数据的安全。

原始数据的安全性

为了保证原始数据的原始性，原始数据一旦保存，便不能被更改；对错误数据只能采取增加一条记录来修正的方式处理，对修正数据应加标志以保证正确性，同时对于修正操作应做数据修正日志，记录修正人相关信息及修正原因等。

防火墙策略

防火墙指的是一个由软件和硬件设备组合而成，在内部网和外部网之间专，用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件，该计算机流入流出的所有网络通信和数据包均要经过此防火墙。