数据库管理制度

版 本 历 史

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 2017-4-19 | 0.1 | 新建 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[**1.** **目的** 3](#_Toc490495072)

[**2.** **数据库级安全管理制度** 3](#_Toc490495073)

[**2.1.** **操作系统口令管理** 3](#_Toc490495074)

[**2.2.** **数据库内部口令管理** 3](#_Toc490495075)

[**2.3.** **密码自身保护** 3](#_Toc490495076)

[**2.4.** **用户（帐号）分类** 3](#_Toc490495077)

[**2.5.** **数据库管理员日常维护管理** 4](#_Toc490495078)

[**2.6.** **数据库管理员授权控制** 4](#_Toc490495079)

[**2.7.** **数据访问控制** 4](#_Toc490495080)

[**3.** **数据库的管理维护方法** 4](#_Toc490495081)

[**4.** **数据库的管理日常工作** 6](#_Toc490495082)

1. **目的**

建立一个在数据库管理维护过程中，相关数据库管理人员可以遵循的安全操作标准。

主要是控制相关工作人员本身的行为规范。需要公司管理部门配合，联合制定一套安全管理制度。包括在界定工作职责（角色）基础之上建立不同级别（权限）的口令。规定不同角色的工作人员不得相互泄露口令等重要安全信息等。

1. **数据库级安全管理制度**
   1. **操作系统口令管理**

在操作系统上的有ROOT权限的用户必须由全部收回，对于一些特殊原因，如研发人员需要下载相关运行日志，需要建立实名的FTP，以及配套的日志下载权限。如果确实需要修改系统内部参数的，都要求研发人员向数据库管理人员申请协同工作，共同修改。数据库管理员会记录下每次协同工作日志和修改日志。

* 1. **数据库内部口令管理**

关键的数据库内部管理用户（root）的口令在数据库创建之初就必须变换默认口令信息。

对于研发而言，需要建立测试数据库环境。对于上线系统，理论上不提供研发人员对数据库的直接访问和修改。

由于java class很容易反编译，建议java class连库的时候要读密码文件。密码文件对用户来说是不读的, 但对java程序来说是可读的。或采用其他方式保护数据库连接所需要的用户的密码信息。

* 1. **密码自身保护**

周期性更换密码（2-3个月），并要求密码具有一定的复杂度（至少6位密码包含数字和字母）

* 1. **用户（帐号）分类**

将数据库的对外操作权限划分成3类帐号：

第1类：应用程序读写数据库的帐号，目前主要通过websphere、tomcat等连接池进行密码配置。此用户及密码只在运维保留。

第2类：工具(tools)帐号，此帐号拥有DML权限，没有DDL权限，主要用于系统内部数据错误等的修改。同时研发部的各个项目组拥有此帐号，可以进行系统内部业务数据的临时处理。（随系统上线运行时间加长，该帐号要被取消）

第3类：开发或维护人员帐号，此帐号拥有只读权限，主要用于维护人员核实、定位客户反映的数据问题等。

* 1. **数据库管理员日常维护管理**

1. 保护数据库内部字典信息

用以保护数据字典不被除拥有SELECT ANY DICTIONARY权限的用户非法查看，或拥有DROP ANY TABLE权限的用户恶意损毁数据字典信息。

1. 所有对上线系统数据库结构的修改均需要由运维完成，日常业务逻辑数据的处理由研发部各个项目组完成(数据库脚本需经过审查通过之后方可执行)
2. 记录用户角色和权限情况，发现有未经核准的异常变动，要立刻汇报上级管理人员，迅速处理安全隐患。
   1. **数据库管理员授权控制**
3. 对数据库用户只授必要权限。要保证具有root的相关权限不授给任何非管理员。
4. 收回不必要的权限或角色。
5. 限制运行时工具授权。
   1. **数据访问控制**

限制数据库所在操作系统的系统用户的数目，用以降低修改默认文件和目录权限的可能性。

1. **数据库的管理维护方法**

数据库系统在信息化建设中的重要地位和作用告诉我们，数据库的日常管理与维护不容小视。为保证数据库数据的安全，应该做到未雨绸缪。

（一）完善管理制度，强化监管力度。数据库系统的安全与企业自身内部的安全机制、内外网络环境、从业人员素质等密切相关。因此，企业应该完善网络系统安全规章制度，防范因制度缺陷带来的风险；企业应该规范操作流程和故障处理流程，减少人为失误与故障，提高故障处理速度，缩短故障处理时间；企业应该通过建立科学合理的责任追究机制，防止出现由于工作态度、工作作风等各种人为因素导致的数据库安全事故。

（二）采取措施，确保数据库数据的安全。保证数据库数据的安全是数据库日常管理与维护工作的首要任务，企业需要采取的安全措施主要有：

（1）网络及操作系统安全。网络系统是数据库应用的外部环境和基础，网络系统安全是数据库安全的第一道屏障。从技术角度讲，网络系统层次的安全防范技术有很多种，大致可以分为防火墙、数字签名与认证、入侵检测等。操作系统是数据库系统的运行平台，能够为数据库系统提供一定程度的安全保护。

（2）操作系统的安全控制方法主要是采用隔离控制、访问控制、信息加密和审计跟踪。主要安全技术有操作系统安全策略、安全管理策略等。

（3）加强用户身份验证。用户身份验证是数据库系统的重要防线。利用窗体身份验证数据库程序的漏洞，进而获取存储在数据库中的用户身份验证密码，这是目前对网络数据库攻击最常见的方式。对此，企业信息部门通常使用带有salt值的单向密码哈希值，以避免用户密码在数据库中以明文形式存储，减轻字典攻击带来的威胁。

（4）对重要数据加密。数据加密交换又称密码学，是计算机系统对信息进行保护的一种最可靠的办法。它利用密码技术对信息进行交换，实现信息隐蔽，从而有效保护信息的安全不受侵犯。数据库加密要求加解密的粒度是每个记录的字段数据。采用库外口加密的方式，对密钥的管理较为简单，只需借用文件加密的密钥管理方法，将加密后的数据块纳入数据库，在算法或数据库系统中做些必要的改动就行。这样有利于公共数据字典的使用和维护系统的完整性。

（5）做好数据库备份与恢复。数据备份是备份数据库某个时刻的数据状态，当系统出现意外时用来恢复系统。依靠网络办公的企业，其信息系统很可能随时被破坏而丢失数据。因此，数据库管理系统必须具备把数据库从错误状态恢复到某一已知的正确状态的功能，这就是数据库的恢复技术。

（三）开展数据库健康检查。为及时发现数据库系统存在的问题，在日常管理与维护中，数据管理员要对数据库开展健康检查。检查内容主要包括以下六个方面

（1）系统环境：操作系统版本、文件系统容量、内存交换区使用率、系统性能。

（2）数据库环境：数据库和补丁版本、是否有僵尸数据库进程、数据库节点数、是否有其他数据库产品及版本。

（3）日志记录。

（4）数据库健康状况：表空间利用率和状态、表空间容器利用率和状态、排序溢出、是否需要收集统计信息、是否需要数据重组、活动日志和日志所在文件系统利用率、死锁发生率、锁升级发生率、锁等待的百分比、编目Cache命中率、包Cache命中率、监视堆利用率、数据库堆利用率、数据库缓冲池命中率。

（5）数据库维护内容：最近一次统计信息收集时间、最近一次表数据重组时间、最近一次绑定包时间、最近一次数据库备份时间。

（6）数据库基本信息记录：数据库内存使用、环境变量。

1. **数据库的管理日常工作**

（1） 每天对数据库的运行状态、 日志文件、备份情况、数据库的空间使用情况、系统资源的使用情况进行检查，发现并解决问题。

（2）每周对数据库对象的空间扩展情况，数据的增长情况进行监控，对数据库做健康检查 , 对数据库对象的状态做检查。

（3） 每月对表和索引等进行 Analyze, 检查表空间碎片，寻找数据库性能调整的机会，进行数据库性能调整，提出下一步空间管理计划。

数据库管理的意义重大，关系到企业信息系统的正常运作，仍至整个企业的生死存亡。要做好数据库的日常管理与维护，不仅要求数据库管理员熟悉掌握专业技术知识，还要有足够的细心和高度的责任心。