数据库安全管理制度

一、目的

为规范数据库系统安全使用活动，降低因使用不当而带来的安全风险，保障数据库系统及相关应用系统的安全，特制定本规范。

二、适用范围

本规范中所定义的数据管理内容，特指存放在信息系统数据库中的数据。

本规范适用于信息系统建设与运维，旨在明确数据库管理员（DBA）工作职责及数据库系统中与安全相关的配置项及其使用要求，指导数据库系统的安装、配置及日常管理，提高信息系统的安全水平。

三、定义

数据库管理员：也称 DBA ，负责数据库安装、调试、使用及日常运维，管理用户对数据库的访问权限，增加、删除、修改该数据库中数据库对象。

DML（data manipulation language）：是SELECT、UPDATE、INSERT、DELETE，就象它的名字一样，这4条命令是用来对数据库里的数据进行操作的语言

DDL（data definition language）：DDL比DML要多，主要的命令有CREATE、ALTER、DROP等，DDL主要是用在定义或改变表（TABLE）的结构，数据类型，表之间的链接和约束等初始化工作上，他们大多在建立表时使用

DCL（Data Control Language）：是数据库控制功能。是用来设置或更改数据库用户或角色权限的语句，包括（grant,deny,revoke等）语句。在默认状态下，只有sysadmin,dbcreator,db_owner或db_securityadmin等人员才有权力执行DCL

四、DBA 职责

1、对数据库系统进行合理配置、测试、调整，最大限度地发挥设备资源优势,负责数据库的安全、稳定运行。

2、对所有数据库系统的配置进行可用性，可靠性，性能以及安全检查。

3、定期对数据库系统的可用性，可靠性，性能以及安全的配置方法进行检查、修订和完善。

4、负责数据库系统运行过程中出现的问题及时处理解决。

5、负责对数据库系统的数据一致性和完整性，并协助开发、网络人员做好相关的配置、检查等工作。

6、负责做好数据库系统及数据的备份和恢复工作。

7、做好数据日常检查记录（CheckList表单）准入要求

4.1.DBA 权限及流程

1、DBA按“1001–信息系统权限申请指南”的规范按纸质流程完成数据库运维账号的申请。

2、DBA 数据库运维账号绑定使用人员设备和手机号码，通过短信或令牌实现2次验证。所有的运维操作通过堡垒机完成，堡垒机记录并审计 DBA 所有的操作指令。

3、禁止远程DDL：核心业务系统限制DDL操作仅能在数据库服务器本地进行，禁止远程连接执行DDL操作。

4、DBA 通过查询分析器执行的数据的变更（包括增加、删除、重建等）操作需和运维部负责人共同评估后通过纸质流程申请执行。

五、安全管理

安全性是数据库重要的日常工作，安全管理的主要内容包括账户管理和权限管理。帐户管理就是在数据库中应该增加哪些帐户、这些帐户应该组合成哪些角色等。权限管理是对象权限和语句权限的管理。

5.1.网络环境安全

1、数据库服务器置于单独的服务器区域，任何对这些数据库服务器的物理访问均应受到控制

2、数据库服务器所在的服务器区域边界部署防火墙或其它逻辑隔离设施。

5.2.服务器安全

1、重要的数据库服务器除提供数据访问服务外，不提供任何其它的服务。如WEB，FTP等。

2、数据库专用帐户，赋予账户除运行数据库服务之外的最小权限，sa或是sysdab等权限不能对外开放。

3、目录及相应文件访问权限进行控制，非管理员不能访问数据库服务器上任何目录如：禁止用户访脚本存放目录。

5.3.数据库安全

5.3.1.数据库系统

1、正式生产数据库系统与开发测试数据库系统物理分离，确保没有安装未使用的数据库系统组件或模块。

2、数据库用户的创建、删除和更改工作，并做好记录。

3、数据库对象存储空间的创建、删除和更改工作，并做好记录。

4、对系统的安装更新、系统设置的更改等要作好维护记录。

5、确保没有开启未使用的数据库系统服务。

6、数据库系统安装必要的升级程序或是补丁，升级前作好数据库备份。

5.3.2.数据保密

严禁任何人泄漏数据库业务关键数据，需要业务数据时，必须向信息总部相关领导提出申请批准后才能对数据进行相关的操作，并做好记录与日志。

数据库安全性设计与管理需要依照《数据保护技术规范》、《数据资产管理条例》等制度实施。

5.3.3.账户设置

1、数据库管理员帐号具有最高数据库管理权限（如：MSSQL的SA或是ORACLE的SYSDBA等），其他人员需要直连访问数据库或需要具有一定数据库操作权限，必须向信息部门相关领导申请，审批通过后，由数据库管理员告知用户权限等信息，其他人员通过业务系统访问数据库。

2、根据业务需要的权限建立专门的账号，以区分责任，提高系统的安全性，业务人员必须使用自己的账号登录数据库,如JOB，存储过程等执行权限。

3、对账号权限的设置遵从最小化原则，不需求的权限就不能开通。如查询数据的人员，只能有对某些表的SELECT权限，而不能用UPDATE，DELETE等权限。

4、普通数据库用户账户与数据库管理员帐户分离。

5.3.4.帐户类型：

- 系统管理员：能够管理数据库系统中的所有组件及所有数据库。
- 数据库管理员：能够管理相关数据库中的账户、对象及数据。
- 数据库用户：只能以特定的权限访问特定的数据库对象，不具有数据库管理权限，大部份都是属于这个用户类型。如业务数据人员。

5.3.5.用户权限

数据库帐户按最小权限原则设置在相应数据库中的权限。下几种权限：

- 系统管理权限：包括帐户管理、服务管理、数据库管理等。
- 数据库管理权限：包括创建、删除、修改数据库等。
- 数据库访问权限：包括插入、删除、修改数据库特定表，视图，过程，FUNCTION，JOB记录等

5.3.6.数据库对象安全

1、数据文件安全，对数据文件访问权限进行控制，如：禁止除专用账户外的其它账户访问、修改、删除数据文件。

2、删除不需要的示例数据库，在允许存在的示例数据库中严格控制数据库账户的权限。

3、删除或禁用不需要的数据库对象，如表，视图，过程，函数，触发器等。

4、敏感数据安全，对于数据库中的敏感字段，如：口令等，要加密保存。

5.3.7.口令密码策略

1、数据库账户口令应为无意义的字符组，长度至少八位，并且至少包括数字、英文字母两类字符。可设置相应的策略强制复杂的口令。

2、必须根据安全要求对数据库管理系统的密码策略进行设置和调整，以确保口令符合要求。

3、定期或不定期修改数据库管理员口令，并与第一条相符合。

4、帐户、密码统一管理，由DBA进行管理，记录帐户变及审核。

5.3.8.访问控制

1、在外围防火墙或其它隔离设施上控制从互联网到数据库系统的直接访问。

2、修改数据库系统默认监听端口。

3、应用程序的数据库连接字符串中不能出现数据库账户口令明文。

4、禁止未授权的数据库系统远程管理访问，对于已经批准的远程管理访问，应采取安全措施增强远程管理访问安全。

5.3.9.帐户开通

1、开通帐户必须先填写“信息系统权限申请指南”，经如下流程人员审批通过后，数据库管理员建立帐号。

2、帐户权限最小化原则。开通只需要的权限，做到不同的应用不同的帐户及专人专帐户。

3、采用OA帐户为数据库开通帐户的基础，可追加"_"符号并设置附加字段（如资源池标记、账户所属组别标记等）。

5.3.10.账户注销

1、数据库管理员收到人员离职通知后，应即时审查该人员是否拥有数据库访问账户；并把对应权限删除。

2、帐户权限最小化原则。开通只需要的权限，做到不同的应用不同的帐户及专人专帐户。

3、采用OA帐户为数据库开通帐户。

5.3.11.MySQL数据库特别设置

1、采用集群配置方案，不得将数据库配置文件部署于数据库本地。配置文件存储服务器的数据安全管控级别应为最高。

2、数据库启动必须采用远程调用配置文件形式启动，不得采用命令行启动，应采用服务调用方式启动，避免通过系统指令查到配置文件所在服务器。

3、应对账户设置白名单策略，针对特殊业务场景可以进行分时段访问拦截。

5.3.12.SQL Server数据库特别设置

1、代理账户宜采用单独账户设置。

2、新业务超过100万行数据的表，必须采用分区表形式实现。

3、数据库必须采用文件组方式实现，每个数据文件不宜超过500GB。

4、tempdb、log与data文件宜硬件IO分离，若资源紧张至少将tempdb与 log和data文件分离。

5、数据库系统文件必须独立存放于系统盘，且与tempdb、log与data文件硬件IO分离。

6、应对账户设置IP白名单策略，针对特殊业务场景可以进行分时段访问拦截。

7、非算法应用场景，可设置资源池分散账户访问压力。

8、减少链接服务器的使用，若必须使用则必须设置账户访问限制，不得提供公共链接服务器访问。

9、DBA存储过程需要部署于system库中，注明sp_dba_前缀，并做好版本控制管理。

10、严格控制标记与指针的使用，在满足性能要求前提下，可将信息写入数据库error日志中，便于后续对接日志处理平台进行集中收集处理。

11、数据库分库分表分区等脚本，必须通过备份库在测试环境执行，评估效率，形成书面报告审议。执行必须按照新建库/表/分区→数据导入→索引重建→名称切换方式进行。涉及视图操作，完成后必须重新刷新视图。分库分表分区后，必须建立维护作业，对函数与方案实现自动维护。正式启用新的分库分表分区前，需要至少2名工作人员对新旧表的数据一致性进行核对，形成书面报告审议，通过后才可启用。被分库分表分区的原始表，需要保留7天。7天后应将该表转移至业务历史数据库留存至少90天。

12、应监控数据库存储过程调用情况，针对超过10个以上的数据库并发访问、链接池资源1个小时内不被释放、CPU和Tempdb资源消耗超过总资源的20%的情况，应作出预警。针对需要特殊保护的业务场景，经产品与运维部门同意，可启动自动切断链接设置。

六、备份与恢复

1、制定数据库系统的备份策略，定期对数据库系统进行备份。如备份周期，方式等。

2、数据库备份策略要以高效备份与恢复为目标，与操作系统的备份最好地结合，物理备份与逻辑备份相结合。

3、必须对备份帐户的权限严格控制，由系统管理员或指定专人负责。

4、妥善存放和保管备份介质（从数据库导出的磁盘柜等），防止非法访问与丢失。

5、本地备份与远程异地备份相结合，以防止本地备份丢失的情况。

6、根据重要性对数据库进行周期或不定期进行恢复测试与应及处理。

7、数据库升级、表结构变更、数据库分库分表分区、业务核心表变更前必须进行数据备份。对数据层面重大调整的，应启动启动完整日志或数据备份等数据容灾策略。

6.1.备份方式及策略

- 完全备份：对备份的内容进行整体备份。
- 增量备份：仅备份相对于上一次备份后新增加和修改过的数据。
- 差异备份：仅备份相对于上一次完全备份之后新增加和修改过的数据。
- 按需备份：仅备份应用系统需要的部分数据，或临时需要解决的问题。

1、建立各个应用能接受的恢复时间和数据备份方式，采取相应的备份策略。

2、结合使用在线备份、逻辑备份和物理备份等多种方式，并且自动方式和手动方式相结合。

3、数据备份应根据系统情况和备份内容，采用不同的备份方式及策略，并做好记录。

6.2.备份要求

1、数据库的数据要求定时自动备份。

2、建立备份记录，详细记录备份数据信息。备份应有明确的文件名，时间点、备份人,备份文件名统一标准。

3、备份文件保存时间可根据数据重要程度和有效利用周期确定。

4、备份介质安全问题，既要保证存放的物理环境，也要避免对备份数据的非授权访问。

5、系统管理员和数据库管理员确定备份策略。

6、备份文件名采用标准格式： 数据库名称 + 下划线 + ISO时间格式（YYYYMMDDHHNNSS,即四位年2位月2位日2位小时2位分钟 + 备份的扩展名bak或是trn（日志文件））

7、数据表的备份命名为原表命名_bak_yyyyMMdd形式命名，若为同一天可以追加批次版本_v1，备份数据宜采用bcp形式进行数据导出与导入。备份表生产环境留存期至少7天。7天后应将该表转移至历史数据库留存至少90天。

6.3.恢复管理

恢复的操作直接影响到实际的应用。恢复操作应严格按一定的操作程序进行，而绝不能由备份系统管理员或某一个应用者进行恢复操作了事。

故障确认。在进行恢复之前首先应该确认造成故障的原因。故障的原因非常多，应该分清是操作系统的故障还是数据库的故障。如果是数据库的故障，不同的数据库应采用不同的故障分析方法，在完成故障分析后确认需要进行恢复操作时，由相应的管理人员提交书面的故障分析报告。

恢复计划。系统管理员在确认故障分析报告后应与相应管理者一起制定详细的恢复计划，包括应恢复的内容、恢复的时间、恢复的操作步骤、恢复对应用造成的影响等，主管领导应确认恢复对生产造成的影响，在批准执行恢复前应以相应方式与有关部门进行沟通和通知有关部门进行恢复前的准备工作。

定期备份校验。对长期保存的备份进行校验，防止在需要时备份不可用的情况发生，使用数据库自带工具校验。