TC260-PG-2025NA

网络安全标准实践指南

——数据库联网安全要求

（征求意见稿 v1.0-202510）

全国网络安全标准化技术委员会秘书处

2025 年 10 月

本文档可从以下网址获得：

www. tc260. org. cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、国家信息技术安全研究中心、中国科学院信息工程研究所、北京安华金和科技有限公司、三六零数字安全科技集团有限公司、天翼云科技有限公司

本文件主要起草人：申任远、王一宇、田文、贾世琳、胡影、刘行、郝春亮、高超、高晨涛、谭峻楠、杨韬、刘曦泽、王哲麟、袁曙光、陈驰、王庆恒、郭亮、刘华林、苏强、吴洋洋

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

数据库和云上对象存储广泛连接至公共网络，在联网过程中和联网状态下面临诸多安全风险，这些风险可能导致数据泄露，对用户隐私、公共利益和国家安全造成严重威胁。

为应对数据库联网过程中和联网状态下的安全风险，本文件从技术要求、管理要求两个方面提出了安全要求，同时也给出了云上对象存储安全要求，旨在减少因安全防护措施不足、安全配置不当、管理不当引发的数据泄露等安全事件。

目　录

1 范围

本文件规定了数据库系统连接至公共网络场景下的安全技术要求、安全管理要求。

本文件适用于指导数据库系统接入公共网络开展数据处理活动，也可为评估机构提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 20273-2019 信息安全技术 数据库管理系统安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

GB/T 25069-2022 界定的以及下列术语和定义适用于本文件。

3.1 数据处理者 data processor

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

[来源：GB/T 43697-2024, 3.11]

4 数据库联网概述

4.1 数据库联网场景概述

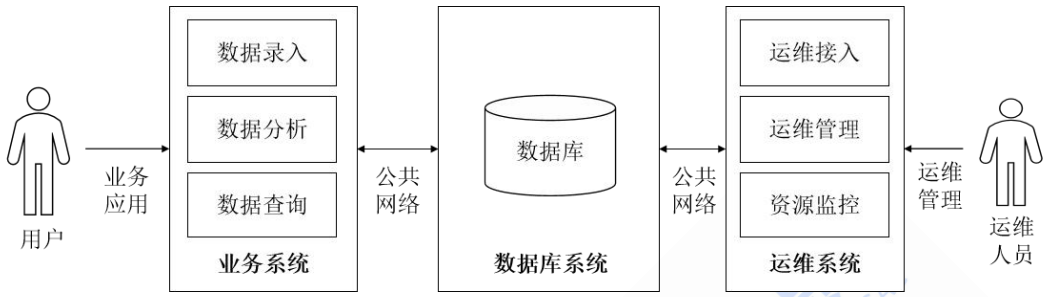

图 1 数据库联网典型场景示意图

图 1 展示了数据库联网的典型场景，包括业务系统、数据库和运维系统三部分。数据库存储业务数据与业务系统、运维系统相连。用户通过业务应用使用业务系统访问数据库。运维人员使用运维系统对数据库进行监控和维护。

4.2 安全要求

本文件将数据库联网安全要求分为安全技术要求和安全管理要求两类。其中，安全技术要求是对数据库在联网环境中应具备的安全功能提出的具体要求；安全管理要求是对数据库联网系统的运行维护、制度建设和人员管理等提出的组织与流程性安全要求。

本文件依据数据库联网业务所处理数据的规模、敏感程度及业务重要性，在遵循 GB/T 22239-2019 的基础上，将数据库联网安全要求划分为以下两个级别：

a）基本级：适用于处理一般数据的数据库联网场景。

b）增强级：符合下列条件之一的数据库联网场景，应满足增强级要求：

1) 处理超过 10 万条个人信息，或超过 1 万条敏感个人信息；

2) 其数据一旦受损，可能导致重大经济损失、广泛社会影响或严重危害国家安全、公共利益；

3) 作为关键信息基础设施的核心组成部分，或支撑国家重要领域的业务运行。

若数据库同时涉及不同级别的数据处理，应依据就高原则，整体满足增强级安全要求。对于增强级特有的要求，在本标准的后续条款中以加粗形式表述。

本文件附录 A 规定了云上对象存储的联网安全要求。数据库联网涉及云上对象存储服务时，除满足正文中的相关要求外，还应符合附录 A 的规定。

5 数据库联网安全技术要求

5.1 身份鉴别

数据处理者使用数据库的身份鉴别安全要求如下：

a) 应修改默认数据库管理员账户密码，密码长度不少于 12 位，包含大小写字母、数字及特殊字符，至少 3 个月更换 1 次；

b) 设备进行用户身份鉴别时提供最少的反馈，应避免提示“用户

名错误”“口令错误”等可能被用于降低口令猜解复杂度的信息；

c) 应建立数据库访问接口（如 JDBC、ODBC）的调用鉴权机制，对接口调用方身份、可执行操作类型及返回数据量进行严格约束。

5.2 访问控制

数据处理者使用数据库的访问控制安全要求如下：

a) 应控制数据库访问接口权限，遵循最小权限原则对不同访问接口的查询范围、查询数量进行限制；

b) 应对数据库配置文件、应用代码以及第三方配置中心（如 Nacos）中的数据库连接账号和密码信息进行加密存储；

c) 应依据业务来源 IP 和应用身份实施精细化访问控制，建立动态数据库连接 IP 白名单机制，仅允许合法应用程序联网访问数据库；

d) 应建立基于角色的访问控制或基于属性的访问控制机制，对数据查询、修改、删除等操作实施行级或列级细粒度权限控制；

e) 应建立通信会话超时重认证机制，并对敏感查询操作实施会话令牌绑定及请求完整性校验；

f) 应设置数据库连接超时自动断开机制，并对失败登录尝试实施阈值控制及锁定策略。

g) 应将数据库管理的权限进行分离，实现特权用户的权限分离，并至少应具备系统管理员、安全管理员和安全审计员。系统管理员负责系统配置、系统运行状态监控等工作；安全管理员负责访问控制、密文传输等安全维护工作；安全审计员负责审计开关的控制、审计数据的查看、审计数据的管理等工作。

5.3 数据加密

数据处理者使用数据库的数据加密安全要求如下：

a) 数据在传输过程中应采用符合 GB/T 39786-2021 第 6.2 条要求的密码技术，保证通信数据的保密性和完整性；

b) 数据在存储时应采用符合 GB/T 39786-2021 第 6.4 条要求的密码技术，实现表级/字段级加密粒度，其中敏感个人信息和重要数据应进行加密存储；

c) 应优先使用国家密码管理部门核准的密码算法（如 SM2、SM3、SM4）和密码产品；

d) 加密密钥宜采用硬件密码模块进行保护，并建立完善的加密密钥生成、存储、分发、轮换与销毁机制；

e) 涉及个人生物识别信息存储时，应采用符合 GB/T 35273-2020 第 6.3 条要求的加密措施，且不得直接存储原始个人生物识别信息。

5.4 边界防护

数据处理者使用数据库的边界防护安全要求如下：

a) 应禁用或限制数据库默认账号的远程网络访问权限；

b) 应更改数据库网络端口为非默认端口，并结合防火墙或安全组限制访问；

c) 应关闭非必需的数据库网络端口与服务，对数据库监听地址进行约束，禁止启用非必需的网络地址及端口；

d) 应对生产环境、测试环境及开发环境实施有效隔离；

e) 应通过堡垒机等中间安全防护设备对数据库进行访问；

f) 应部署边界防护设备，仅开放数据库的必要端口与协议；

g) 应部署数据库防火墙，设置安全策略并定期更新规则；

h) 应在网络边界部署数据库通讯协议深度解析与访问控制设备，对异常连接请求、高频次查询及大规模数据抽取行为进行实时监测与阻断。

5.5 网络传输

数据处理者使用数据库的网络传输安全要求如下：

a) 数据传输过程中应使用通信加密协议（如 SSL、TLS 等），并需及时更新通信加密协议的版本，以应对相关协议的已知安全漏洞问题；

b) 应对密钥进行安全存储，不应将使用密钥在代码中硬编码或明

文存储；

c) 对于跨不同安全域的数据传输，应建立安全或专用传输链路，并对输出数据实施脱敏处理；

d) 涉及大量个人信息数据跨境传输的数据库，还应满足国家关于数据出境安全评估的相关要求。

5.6 日志审计

数据处理者使用数据库的日志审计安全要求如下：

a) 应记录并审计所有数据库联网访问行为，包括但不限于用户身份、操作时间、源 IP 地址、目标数据库对象（如表、字段）、操作类型（如 SELECT、UPDATE、DROP）、操作结果（成功或失败）及具体操作内容；

b) 应具备日志查询和分析能力，并满足：

1）仅允许授权管理员访问审计日志；

2）可根据日期、时间、用户标识等条件进行组合搜索；

3）审计日志可以清空和导出。

c) 日志审计模块应具备严格的访问控制与完整性保护机制，采用独立部署的审计设备或专用管理网络，确保审计日志不可非法删除、篡改或绕过；

d) 应将审计日志存储于掉电非易失性存储介质中，且保存时限不能低于 6 个月；

e) 应对日志审计模块采取安全保护措施，宜采用独立于数据库服务器部署的数据库审计设备，并定期备份日志；

f) 应定期对审计策略有效性进行评估，并根据业务变化和数据敏感性动态调整审计范围与告警阈值。

6 数据库联网安全管理要求

6.1 运维管理

数据库的运维管理要求如下：

a) 应建立数据库远程运维操作审批与监控流程，所有远程运维会话须经过授权并实施全程记录与动态监测；

b) 应对数据库的开发和运维人员进行行为监督和审计，进行运维账号的集中管理与权限分离，禁止共享运维账号，并依据职责为运维人员分配最小必要权限；

c) 数据库上线前应对照安全技术要求进行安全评估；

d) 应建立数据库变更管理制度，对结构变更、数据批量更新、权限调整等操作实行申请、审批、执行与复核相分离的机制；

e) 应严格隔离数据库开发、测试与生产环境，禁止直接使用生产数据用于非生产环境，确需使用时应进行脱敏或去标识化处理；

f) 应定期识别数据库访问接口（包括 API、中间件及应用程序直连等），并对接口的认证、授权与审计策略进行审查和优化。

6.2 合作外包管理

数据库的合作外包管理要求如下:

a) 应与合作方通过具有法律效力的合同、协议或工作说明书等形式，明确其在数据库访问、使用、存储、传输及销毁各环节的安全保护责任、技术措施要求和违约责任;

b) 应建立合作方数据库安全能力评估与准入机制，对其身份鉴别、访问控制、安全审计、数据防护和应急响应等方面的技术和管理能力进行审核与定期复查;

c) 应要求数据合作方建立与其数据处理规模和安全风险相匹配的数据库安全管理机制;

d) 合作方涉及数据出境或跨境提供时，应事先开展安全评估并依法报请主管部门审批，且数据传输与存储环节须满足国家关于数据出境的合规要求;

e) 发生数据库安全事件或发现重大安全风险时，应及时向合作方和监管方通报，并立刻采取处置措施，消减危害影响。

6.3 人员管理

数据库的人员管理要求如下:

a) 应建立健全数据库操作岗位责任制，明确不同岗位人员在数据安全生命周期内的职责与操作权限边界;

b) 应实施严格的数据库权限审批与分配流程，基于最小权限原则

为不同角色分配系统管理、数据访问及运维操作权限，禁止权限过度授予；

c) 应定期对数据库相关人员的权限进行审查和调整，根据人员岗位变动、职责调整及离职转岗等情况，及时更新权限设置；

d) 应建立关键岗位人员安全背景审查机制，对数据库管理员及可访问敏感数据的人员实施岗前审查与在岗定期复审；

e) 应实现数据库操作人员身份与操作行为的唯一标识和不可否认性，推广采用多因素认证、动态令牌或生物特征等强身份鉴别机制；

f) 应建立并落实数据库高风险操作（如批量数据导出、权限变更、数据删除等）的双人复核与审批制度，并对操作过程进行全程审计跟踪；

g) 应对第三方外包人员的数据库操作实施额外管控，包括签订保密协议、限制访问范围、操作行为全程监控及审计日志独立留存。

6.4 供应链管理

数据库的供应链管理要求如下：

a) 应在采购数据库产品及关联服务前，对供应商的安全开发能力、产品历史漏洞情况、应急响应水平及持续维护保障能力进行综合评估与验证；

b) 应在采购数据库相关产品时，符合 GB/T 20273-2019 第 7.3 节提出的安全保障要求，明确产品的安全要求、安全更新保障、漏洞响应时限等，确保产品在全生命周期内的安全性；

c) 应在采购合同或技术协议中明确供应商的安全责任和义务，包括但不限于漏洞响应与修复时效、安全更新支持周期、数据安全保护承诺及违约责任；

d) 应建立数据库产品与组件的软件物料清单（SBOM）管理机制，确保所有第三方库、驱动及依赖组件来源可信、版本可溯，并无已知高危安全漏洞；

e) 应定期对数据库供应链的安全状况进行审查和评估，及时发现并处置供应链中存在的安全风险，必要时调整供应商；

f) 应制定数据库供应链安全事件应急预案，明确在供应商服务中断、产品停维、漏洞未及时修复等场景下的应急处理流程与技术措施。

附 录 A

（规范性）

云上对象存储安全要求

本附录给出云上对象存储的安全要求。

A.1 账号与访问管理

A.1.1 账号分级与权限管理

云上对象存储在账号分级与权限管理方面，应满足以下要求:

a) 严禁使用主账号进行日常操作，应创建子账号，并依据最小权限原则分配相应权限。

b) 针对高权限子账号（如具备系统管理员、安全管理员等高权限角色）及高危操作（如删除数据库、修改重要权限、批量删除等），应设置访问条件控制，并结合多因素认证（MFA），如短信验证码、硬件令牌等方式，对敏感操作进行二次认证。

c) 避免硬编码 AK/SK，防止凭证泄露。

d) 建立定期审计机制，对用户权限及登录信息进行审查。

A.1.2 访问策略配置

云上对象存储在访问策略配置方面，应满足以下要求:

a) 存储空间访问策略应遵循权限最小化原则，避免授权整个存储空间，若需授权，应精确到具体对象或对象前缀。

b) 严格限制匿名访问。除特殊情况并经过专门评审外，应确保所

有访问均通过身份验证和授权进行。

c) 在存储空间的操作权限配置中，严格配置业务需求中必需的接口权限。如应用仅需对对象进行读取操作，则仅配置读取权限。

A. 2 数据加密

A.2.1 传输加密

云上对象存储在数据传输加密方面，应满足以下要求:

a) 使用网络加密协议进行数据传输。匿名用户对目标存储空间内资源的所有请求访问应强制设置为高安全加密（如 HTTPS）方式。

b) 定期更新和检查 SSL/TLS 证书。

A.2.2 存储加密

云上对象存储应启用服务器端加密，确保数据在静态存储时处于加密状态。

A. 3 数据保护与备份

A.3.1 对象锁定

对于重要数据和核心数据，应启用对象锁或确保在设定的有效期内，存储桶内相关数据处于只读状态，不可进行覆写或删除操作。

A.3.2 版本控制

云上对象存储应开启版本控制功能，确保文件不会被意外覆盖或删除。

A.3.3 数据备份与容灾

云上对象存储宜利用存储桶复制功能，将数据复制到其他区域的数据中心，实现异地容灾。

对于数据持久性要求苛刻，且数据主要存储在其他云厂商的客户，可采用多云灾备方案。

A. 4 安全监控与审计

A.4.1 事中监控

基于云函数等技术，针对高危操作（如删除文件、修改重要权限等）配置事件通知，在操作发生时，立刻向管理员邮箱或手机发送通知，以便及时发现并采取措施中止高危行为。

A.4.2 事后审计

启用存储桶访问日志功能，对用户访问操作（如删除文件、覆盖写文件、修改文件权限等）进行记录和追踪。

A. 5 其他安全措施

A.5.1 防盗链设置

配置防盗链设置，对访问来源进行白名单或黑名单管理，避免对象存储资源被未经授权的第三方盗用。

A.5.2 跨域资源共享（CORS）配置

合理配置 CORS 规则，防止因不合理的跨域配置导致的数据泄露风险。

A.5.3 文件命名策略

避免使用顺序前缀（如时间戳、字母顺序、日期、数字 ID 等可被遍历的方式）命名文件。建议在文件名中添加十六进制哈希前缀或以反转文件名等方式命名，降低文件名被攻击者遍历获取全部文件的风险。