ICS XXXXXXX
CCS X XX

DB65

新 疆 维 吾 尔 自 治 区 地 方 标 准

DB65/T XXXX-2024

一体化数据资源体系
数据安全体系建设指南
（征求意见稿）

2024-XX-XX 发布　　2024-XX-XX 实施

新疆维吾尔自治区市场监督管理局　　发 布

目　次

前　言

本标准按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规则编制。

本标准由新疆维吾尔自治区数字化发展局提出并归口。

本标准主要起草单位：新疆维吾尔自治区数字化发展局。

本标准主要起草人：

一体化数据资源体系数据安全体系建设指南

1 范围

本文件提出了数据安全体系要求，主要包括数据安全体系架构、数据安全管理体系、平台技术防护、数据安全运行管理要求。

本文件适用于政务部门以及参与数据处理活动的相关组织开展数据安全体系规划、建设、管理、评估与监督。

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 信息安全技术 术语

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

3 术语与定义

GB/T 25069 界定的术语和定义及下列术语和定义适用于本文件。

3.1

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.2

数据全生命周期 data life cycle

包括数据采集、传输、存储、使用、共享、销毁等各个关键环节。

3.3

敏感数据 sensitive data

由权威机构确定的受保护的信息数据。

3.4

数据血缘关系 data lineage

数据在产生、处理、流转到消亡的过程中，数据之间形成的可回溯的关联关系。

3.5

数据溯源 provenance information

数据处理过程中记录的可实现追踪数据来源的信息。

4 数据安全体系架构

数据安全体系包括数据安全管理体系、平台技术防护、数据安全运行管理三个部分，体系架构如图1所示。

图 1 数据安全体系架构

5 数据安全管理体系

5.1 基本要求

数据安全管理体系应覆盖数据采集、传输、存储、加工、共享、开放、销毁等数据全生命周期关键环节。

5.2 数据分类分级管理制度

数据分类分级管理制度内容主要包括：

a） 数据分类分级原则、分级要素、分级规则；

b） 数据分类分级操作指南和分级流程；

c） 不同级别的数据安全管理要求；

d） 数据级别的变更场景、变更申请审批流程等。

5.3 数据访问权限管理制度

数据访问权限管理按照角色权限制约和赋予用户开展工作所必须最小权限的原则，内容主要包括：

a） 数据访问权限安全管理职责分工；

b） 数据访问权限的账号分配、开通、使用、变更、重置、锁定、注销等审批流程要求；

c） 人员岗位变动后，访问账号权限变更流程等。

5.4 数据脱敏管理制度

数据脱敏管理制度可基于数据级别及应用场景，结合实际需求制定，内容主要包括：

a） 数据脱敏原则和方法；

b） 数据脱敏工作流程；
c） 数据脱敏工作的管理要求；
d） 数据脱敏工作的技术要求等。

5.5 数据开放共享管理制度

数据开放共享按照履职需要和最小化原则，内容主要包括：
a） 数据开放共享的范围、内容；
b） 数据开放共享的申请、审批等工作流程；
c） 数据开放共享安全管理要求；
d） 数据开放共享安全技术要求等。

5.6 数据安全销毁管理制度

数据安全销毁管理制度应充分考虑数据销毁与删除的必要性、及时性、可靠性等，内容主要包括：
a） 各级别数据销毁对象；
b） 各级别数据销毁场景；
c） 各级别数据销毁方式；
d） 各级别数据销毁流程；
e） 各级别数据销毁工作要求等。

5.7 安全应急处置制度

通过数据安全应急处置制度，及时应对数据安全事件，减少数据安全事件所带来的不利影响，内容主要包括：
a） 数据安全事件分类分级方法；
b） 数据安全事件主体责任和应急处置机制；
c） 各级别数据安全事件发现、上报、处置、溯源、总结等工作流程；
d） 各级别数据安全应急预案编制及应急演练的工作要求等。

5.8 安全日志审计制度

制定数据安全审计制度，通过数据处理活动各环节的日志采集及分析，识别数据安全风险，提供发生安全事件时的追溯取证能力，内容主要包括：
a） 数据安全审计策略、对象、内容、周期等；
b） 数据安全审计日志标准化要求；
c） 数据安全审计日志的采集内容、采集方式、存储要求；
d） 数据安全审计报告的编写、审计问题跟踪要求等。

5.9 安全监督检查制度

数据安全监督检查制度内容主要包括：
a） 数据安全管理监督检查范围、内容；
b） 数据安全管理监督检查方式、措施；
c） 数据安全管理监督检查工作周期；
d） 数据安全管理监督检查工作流程等。

6 平台技术防护

6.1 基本要求

平台技术防护应覆盖数据全生命周期各环节，防止数据泄露、篡改、滥用及毁坏等风险。

6.2 全生命周期安全防护技术

依据场景按需建立数据全生命周期各环节对应安全保障措施，监测和防范可能存在的安全风险，包括但不限于数据篡改、泄露、滥用、损毁等。数据全生命周期安全防护技术主要包括：

a） 在数据采集阶段，包括数据源统一鉴别技术、敏感数据识别技术、数据分类分级标识技术、数据测绘技术等；
b） 在数据传输阶段，包括数据加密技术、传输通道加密技术等；
c） 在数据存储阶段，包括数据备份恢复技术、数据加密存储技术等；
d） 在数据使用阶段，包括数据脱敏技术、数据防泄漏技术、数据血缘关系技术等；
e） 在数据共享阶段，包括数据水印技术、区块链技术、隐私计算技术等；
f） 在数据销毁阶段，包括数据有效销毁技术、销毁数据识别技术等。

6.3 安全态势感知技术

利用异常行为检测、聚类分析、深度学习等大数据分析方法，建立安全态势预警模型，对数据的安全趋势、潜在的安全风险进行趋势分析和预警，及时对安全事件进行处置。安全态势感知技术主要包括：

a） 数据采集技术；
b） 数据处理技术；
c） 数据存储技术；
d） 安全态势分析技术；
e） 数据安全威胁的发现和识别；
f） 态势预警和处置建议；
g） 数据画像和用户行为画像技术；
h） 可视化展示技术等。

6.4 访问权限管理技术

采用访问权限控制管理技术，确保仅赋予用户开展工作所必须的最小权限。数据访问权限管理技术主要包括：

a） 数据访问权限集中身份认证技术；
b） 数据访问权限统一入口访问控制；
c） 基于终端、网络、系统、文件、数据库表及字段等级别的访问控制技术等。

6.5 数据开放共享安全技术

公共数据开放共享安全技术主要包括：

a） 符合 GB/T 39477 中的安全要求；
b） 数据资源提供部门采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性；
c） 数据资源提供部门对开放共享的数据采取数字水印、区块链等技术，确保共享数据可溯源；
d） 采用数据隐私计算技术实现数据开放共享的安全性等。

6.6 密码管控技术

为各类应用及业务提供全方位的密码技术应用支撑。密码管控技术主要包括：

a） 数据加密；
b） 密钥管理；

c） 时间戳服务；
d） 密码运算服务等。

7 数据安全运行管理

7.1 基本要求

基于制度规范和平台技术防护，从人、数据、场景等维度，建立数据安全运行管理体系，实现数据合规、安全的流动及使用。

7.2 安全管理团队

数据安全组织保障是数据安全体系建设的基础，负责控制组织数据安全管理目标的实现。数据安全管理团队构成及职责主要包括：

a） 数据安全管理者：对组织的数据安全负责的个人或团队。组织建立数据安全体系，负责数据安全工作的总体监管、协调与重大事项决策；
b） 数据安全执行者：负责数据安全管理工作的执行，落实各项安全措施，配合数据安全管理者开展各项工作；
c） 数据安全审计者：对数据安全管理工作进行监督、检查和审计，落实数据安全监督检查机制。

7.3 安全服务管理

建立日常安全防护能力评估及测试，有效提升安全防护能力。安全服务管理主要包括：

a） 渗透测试；
b） 安全漏洞扫描；
c） 风险评估；
d） 重保支撑；
e） 等级保护测评；
f） 攻防演练；
g） 安全投诉响应等。

7.4 安全教育培训

数据安全教育培训机制主要包括：

a） 明确各岗位人员安全责任；
b） 定期针对数据安全岗位人员开展数据安全教育培训；
c） 定期针对所有岗位人员开展数据安全教育培训；
d） 对教育培训结果实施考核，确保培训的效果等。

7.5 安全应急处置

数据安全事件应急处置机制主要包括：

a） 建立数据安全事件应急处置机制，编制应急预案；
b） 当发生数据安全事件时，立即启动应急预案，采取相应的应急处置措施，并按照有关规定向主管部门报告；
c） 按照应急预案要求开展应急演练，每年至少一次；
d） 根据实际情况变化，优化应急预案等。

7.6 数据安全审计

数据安全审计机制主要包括：

a） 数据安全审计覆盖数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据销毁与删除等数据处理活动各环节，明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求；

b） 对数据处理活动环节实施日志留存管理，在发生安全事件时可提供数据溯源取证能力，日志保存时间不少于三年；

c） 定期对数据处理活动各环节日志进行数据安全审计，每年至少一次，形成数据安全审计报告；

d） 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.7 安全监督检查

数据安全监督检查机制主要包括：

a） 对敏感数据、特权账号、基础设施等安全管理工作落实情况进行检查；

b） 建立安全监管问题通知和整改流程；

c） 采用人工或自动的实现方式等。

参 考 文 献

[1] 《国务院办公厅全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102号）

[2] 《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）

[3] 《自治区数字政府改革建设方案》

[4] 《自治区数字政府建设三年行动计划（2023-2025年）》

[5] 《新疆维吾尔自治区标准化条例》

[6] 《新疆维吾尔自治区公共数据管理办法（试行）》