ICS 35.04
CCSL80

DB53

云　南　省　地　方　标　准

DB53/T 1403—2025

网络安全等级保护
数据安全治理体系建设指南

2025 －05－09发布　　2025－08－09 实施

云南省市场监督管理局　　发布

前　言

本文件按照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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由云南省公安厅提出并归口。

本文件起草单位：云南警官学院、云南南天电子信息产业股份有限公司、云南省市场监管局信息中心、云南省医疗保障基金运行监测评估中心、云南省康旅控股集团有限公司。

本文件主要起草人：万晋华、屈旻、周子云、徐杨子凡、李朴楠、贺韬、江悦、杨衍、段松、董志文。

网络安全等级保护　数据安全治理体系建设指南

1　范围

本文件给出了数据安全治理体系建设的基本原则、治理框架、基础通用、数据安全管理、数据安全技术、数据安全运营等内容。

本文件适用于指导非涉密数据安全治理体系建设工作，也可供数据处理活动的开展参考使用。

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 22239 信息安全技术网络安全等级保护基本要求

GB/T 25069 信息安全技术术语

GB/T 37988 信息安全技术数据安全能力成熟度模型

GB/T 41479 信息安全技术网络数据处理安全要求

GB/T 43697 数据安全技术数据分类分级规则

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不可泄露的性质。

[来源：GB/T 25069-2022,3.41]

3.2

数据完整性 data integrity

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变

[来源：GB/T 25069-2022,3.574]

3.3

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069-2022,3.345]

3.4

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

[来源：GB/T 25069-2022,3.196]

4 基本原则

4.1 合规正当

宜确保数据全生命周期各环节数据活动的合规性和正当性。

4.2 目的明确

宜制定数据安全防护策略，明确数据全生命周期各环节的安全防护目标和要求。

4.3 全程可控

宜采取与数据安全级别相匹配的安全管控机制和技术措施，确保数据在全生命周期各环节的保密性、完整性和可用性，避免数据在全生命周期内被破坏、篡改、泄漏、丢失或未授权访问等。

4.4 动态控制

数据的安全控制策略和安全防护措施，宜基于业务需求、安全环境、用户行为等因素动态调整。

5 治理框架

数据安全治理体系框架如图1。

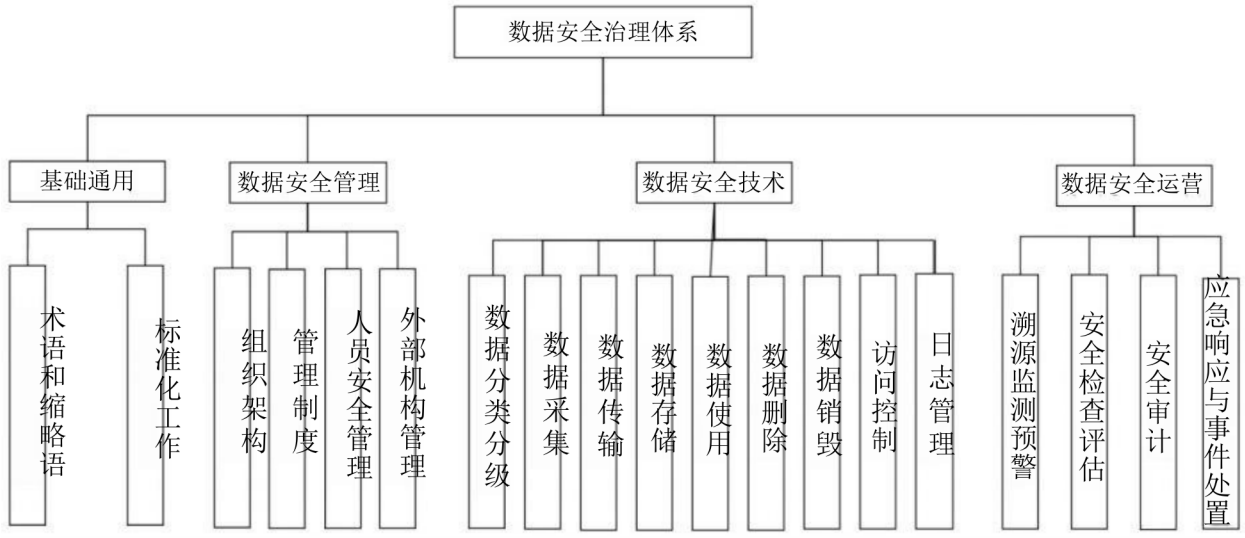

图 1 数据安全治理体系框架图

6 基础通用

基础通用包括术语和缩略语、标准化工作等内容，宜遵循GB/T 25069、GB/T 22239等的相关要求。

7 数据安全管理

7.1 组织架构

宜建立自上而下的覆盖决策、管理、执行、监督四个层面的组织架构，主要内容如下：

a) 决策层主要包括数据安全工作的统筹组织、指导推进和协调落实；

b) 管理层主要包括数据安全相关工作的实施、相关政策和制度的制定评审、设立岗位职能职责、保障工作资源；

c) 执行层主要包括落实数据安全防护措施、数据权限分配、数据安全控制、配合执行数据相关安全评估及技术检测、制定数据安全应急预案、处置安全事件、记录数据活动日志；

d) 监督层主要包括安全审计、监督数据安全政策的执行、受理数据安全和隐私保护相关投诉和举报、配合开展外部审计。

7.2 管理制度

7.2.1 宜制定数据安全总体安全策略、方针、目标、原则，并定期评估和更新。

7.2.2 宜制定数据分类分级原则、要求和工作程序，并定期评估和更新。

7.2.3 宜建立统一覆盖数据全生命周期关键环节的数据安全管理制度及实施细则，并定期评估和更新，主要包括：

a) 制定数据安全管理规定，提出本机构数据安全生命周期保护工作的总体策略；

b) 针对不同安全级别的数据，制定相应的安全策略和保障措施；

c) 建立数据安全日常管理及操作流程，对数据生命周期各阶段的数据保护工作提出具体要求；

d) 建立合理、统一的密码使用和密钥管理技术规范和制度；

e) 建立数据脱敏技术规范和制度，明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制，及脱敏操作过程留存日志记录规范；

f) 建立数据供应方安全管理要求，明确管理内容、方式等；

g) 建立数据采集、传输、存储、使用、删除及销毁相关管理制度；

h) 制定数据采集的操作规程，规范数据采集的渠道、数据格式、流程和方式；

i) 建立数据安全评估、个人信息安全影响评估以及内外部数据安全检查与评估制度；

j) 建立数据安全事件管理、处置规程和应急响应等机制，明确重大数据安全事件的处置流程及应对方法。

7.3 人员管理

7.3.1 建立人员录用及日常管理制度，主要包括录用员工背景调查、保密制度、岗位职能职责、岗位变动要求、终止劳动合同要求、外部人员管理制度等。

7.3.2 制定数据安全相关岗位人员的安全培训制度，主要包括培训计划、培训规程、培训结果评价、培训考核等。

7.3.3 宜对接触高安全等级数据的人员及其岗位建立审批、登记、定期审查管理制度。

7.3.4 数据库管理员、操作员及安全审计人员等岗位宜设立专人专岗制度，数据安全关键岗位宜建立双人双岗制度。

7.4 外部机构管理

7.4.1 宜对参与本机构数据全生命周期过程中的外部机构进行管理，建立相关管理体系。

7.4.2 建立外部机构管理制度，包括但不限于建立外部机构审查与评估机制、外部机构数据使用行为约束机制、外部机构及人员安全要求、定期检查制度、数据安全事件反馈机制等。

7.4.3 宜对接入和涉及的外部产品和服务建立数据安全管理制度，明确接入基本条件，规定所需的数据安全保护能力要求，并制定数据处理、安全性验证、活动监视及安全事件处置等相关规范。

8 数据安全技术

8.1 数据分类分级

8.1.1 宜根据本机构所属行业的数据及其属性或特征制定数据分类作业指导书。

8.1.2 宜根据本机构所属行业数据敏感程度及其在遭受篡改、破坏、泄露或非法利用后可能对个人、组织或国家安全造成的影响制定数据分级作业指导书。

8.1.3 数据的分类分级方法宜按照GB/T 43697及所属行业的数据分类分级的相关规定执行。

8.2 数据采集

8.2.1 宜明确数据采集过程中个人和重要数据的知悉范围和安全管控措施，确保采集数据的合规性、完整性和真实性。

8.2.2 宜与数据所有方签订纸质或者电子的合同协议，合同协议中明确隐私保护政策及约定的采集范围范围、频度、类型、用途。

8.2.3 通过纸质表单采集数据并转换为电子数据时，宜对表单的保存、查阅、复制流转的全过程进行监控与审计，采取技术措施对电子化过程中的数据完整性、保密性进行控制。

8.2.4 数据采集还宜符合GB/T 41479中5.2的要求。

8.3 数据传输

8.3.1 宜采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性。

8.3.2 宜采用密码技术或非密码技术等方式，确保数据传输的完整性和保密性。

8.3.3 宜保障数据传输终端或工具的安全性，终端或工具上线前开展必要的准入控制、终端鉴别、渗透测试等工作，防止未授权终端或工具接入内部网络。

8.3.4 通信双方进行身份认证，宜采用数字签名、时间戳等方式，确保数据传输的抗抵赖性。

8.4 数据存储

8.4.1 数据存储宜根据安全级别、重要性、量级、使用频率等因素，将数据分域分级存储，并采用最小够用原则存储数据，国家及行业主管部门另有规定的除外。

8.4.2 宜根据数据的安全级别和数据对系统运行的影响，制定数据备份和恢复策略。

8.4.3 有条件的宜建立同城与异地数据备份中心，并实现远程数据备份与恢复功能。

8.4.4 宜定期开展数据存储及过程的风险评估，动态完善风险防控措施。

8.4.5 宜定期开展灾难恢复演练，动态调整备份和恢复策略。

8.5 数据使用

8.5.1 宜结合数据主体角色、业务需求及时效性，遵循最小够用原则，设定数据访问权限规则。

8.5.2 宜根据数据分类分级结果，制定和明确数据访问控制过程中的相关安全措施，保障数据在访问过程中的保密性和完整性。

8.5.3 宜每半年进行一次数据的访问权限和实际访问控制情况审计。

8.5.4 宜根据最小够用原则，明确数据导出场景、导出数据范围及相应权限规则。

8.5.5　数据导出宜有明确的权限申请和审核批准机制，并配备安全、完善的实名身份验证措施。

8.5.6　数据导出宜留存记录，其留存时间不少于6个月。

8.5.7　宜明确原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全及处理结果安全等要求。

8.5.8　数据加工之前宜进行数据安全评估，并采用加密、脱敏等技术措施保障加工过程的数据安全性。

8.5.9　宜对数据加工过程进行必要的监督和检查，确保加工过程的数据安全性，并完整记录数据加工过程的操作日志

8.5.10　数据展示前，宜事前评估展示需求，包括展示的包括展示条件、环境、权限、内容等，确保展示的必要性和安全性。

8.5.11　数据展示时宜符合如下要求：

a)　展示界面增加水印，包含访问主体、访问时间等信息；

b)　不使用用展示界面的复制、打印等功能，防止数据导出；

c)　业务系统对数据明文查询实现逐条授权、逐条查询，或具备查询相关监测预警功能，并留存查询日志。

8.5.12　开发测试宜符合以下要求：

a)　实现开发测试环境数据与生产环境数据的有效隔离；

b)　使用经审批授权的安全运维管理平台或数据提取专用终端获取数据；

c)　开发测试过程中产生的数据事先进行脱敏处理，防止数据泄露，除非国家及行业主管部门另有规定；

d)　使用外部软件开发包、组件、源码等前进行数据安全评估；

e)　制定开发测试安全审核流程，对数据源、需求进行审核，确保数据分析的正当性与合法性；

f)　对开发测试过程进行日志记录，并定期进行安全审计。

8.5.13　宜依法依规对外公开披露数据。

8.5.14　数据公开披露前，宜对拟披露数据的合规性、业务需求、数据脱敏方案进行审核，确认披露渠道、披露时间、拟公开数据的真实性及数据脱敏效果。

8.5.15　依据机构有关程序执行数据公开披露审批程序，并留档审批过程和记录。

8.5.16　原则上不宜转让数据，除非满足国家与行业主管部门要求、已获得数据转让相关授权或在机构收购、兼并、重组等情形下依照规定履行义务。

8.5.17　因机构收购、兼并、重组等情况发生数据转让时，宜履行告知义务，并确保承接机构继续履行数据安全保护责任；如变更数据使用目的，宜重新获得个人信息主体的明示同意或授权。

8.5.18　委托第三方机构处理数据的，第三方机构宜符合以下要求：

a)　具有相应资质，并进行事前尽职调查；

b)　委托行为不超出已获授权及合同约定的数据使用范围；

c)　对数据委托处理行为进行数据安全影响评估，涉及个人信息的宜进行个人信息安全影响评估，并采取有效保护措施；

d)　对被委托方的数据安全防护能力进行评估，确保其具备足够的数据安全防护能力。

8.5.19　在数据共享前，宜开展数据安全影响评估，评估共享的数据内容、范围、时间周期、传输方式、用途、安全管控手段等要素，涉及个人信息的不宜超出其授权范围，确保数据安全保护强度不因数据共享而降低。

8.5.20　宜对数据共享过程留存日志记录，包括共享内容、共享时间、防护技术措施等信息。

8.6　数据删除

8.6.1 宜约定数据保存期限，对超过保存期限的数据进行删除。

8.6.2 用于开发测试、数据分析等需求的数据，宜在使用完后进行数据删除处理，记录数据删除处理过程，并及时反馈数据删除处理结果。

8.6.3 宜及时开展数据删除的有效性复核和数据删除处理结果确认。

8.7 数据销毁

8.7.1 宜制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施。

8.7.2 不再使用的存储数据的介质宜采用物理损坏的方式进行销毁处理；使用中的存储介质宜通过多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或者以其他形式被利用。

8.7.3 宜开展数据销毁效果评估，定期对数据销毁效果进行确认。

8.8 访问控制

8.8.1 宜符合GB/T 41479中5.2的要求外，同时满足以下要求：

a) 依据“业务必需、最小权限、职责分离”的原则，确定最小访问权限；

b) 配置用户访问控制策略，实现身份标识与鉴别。

8.9 日志管理

8.9.1 宜开展数据全生命周期记录，形成日志记录，日志记录包括但不仅限于日期和时间、事件类型、主体身份、事件内容、事件结果等。

8.9.2 宜对日志记录进行安全保护，定期开展日志记录审计，防止未授权的访问和输出，确保日志记录的安全。

8.9.3 日志记录宜留存不少于6个月。

9 数据安全运营

9.1 溯源监测预警

9.1.1 宜制定数据溯源的策略和机制，建立数据资产地图，对数据对象进行标记和跟踪，构建和维护数据血缘关系，标识数据的来源合法性，评估数据质量。

9.1.2 宜构建数据溯源的安全模型，增强数据操作的可追溯性。

9.1.3 宜采取数据流量分析技术对数据采集、传输、存储、使用和分析等关键节点进行监测，监测内容包括但不仅限于流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向、异常行为、传输和下载等信息。

9.1.4 宜建立数据安全预警体系，通过安全设备、探针等技术手段，对影响数据安全的事件进行识别、发现、跟踪、监控和告警。

9.2 安全检查评估

9.2.1 宜建立数据安全检查评估机制，定期制定数据安全检查评估计划。

9.2.2 当国家及行业主管部门的相关要求发生变化，或产品和服务发布前，或业务功能发生重大变化时，宜进行数据安全评估。

9.2.3 每年至少宜开展1 次数据安全检查评估，形成数据安全评估报告，评估方式包括但不限于自评估、外部第三方机构评估等。

9.3 安全审计

9.3.1 宜制定安全审计规范，明确安全审计范围和审计人员。

9.3.2 宜定期开展安全审计，形成安全审计报告。

9.4 应急响应与事件处置

9.4.1 宜制定应急响应规范，建立完善的应急响应和问责机制，并制定详细的应急预案，明确应急响应流程、责任分工和处置措施，确保在紧急情况下重要信息资源的可用性和业务连续性。

9.4.2 每年宜定期开展应急演练，检验应急预案的有效性和可行性，分析和总结应急演练中存在的问题和解决思路。

9.4.3 宜制定事件处置规范，分级管理安全事件，制定安全策略，对不同级别的安全事件进行相应处置，重大事件发生后应及时启动应急响应机制。

9.4.4 宜在事件处置结束后，分析和总结原因和存在的问题，形成调查记录、事件清单和总结报告，根据事件分析结果调整数据安全策略，完善应急预案，避免事件再次发生。