ICS 35.040
CCS L 80

DB4401

广　州　市　地　方　标　准

DB4401/T 276—2024

网络数据安全管理规范

Network data security management specification

2024-08-28 发布　　2024-09-28 实施

广州市市场监督管理局　　发布

目　　次

前　言

本文件按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这些专利的责任。

本文件由广州市互联网信息办公室提出并归口。

本文件起草单位：广州市信息安全测评中心、广州市标准化研究院、北京安华金和科技有限公司、中电科网络安全科技股份有限公司、广州赛西标准检测研究院有限公司、杭州安恒信息技术股份有限公司、奇安信网神信息技术（北京）股份有限公司、广东华进律师事务所、中国联合网络通信有限公司广州市分公司、广州绿盟网络安全技术有限公司。

本文件主要起草人：陆志强、贺忠、鲁胜兵、施冰、王冰、曾剑锋、徐湛、魏力、吴杨松、刘柳妹、王龙、颜爱军、宋常林、楚赟、程珂昵、晁静洋、陈朝华、彭冕莉、余清霞。

网络数据安全管理规范

1 范围

本文件给出了网络数据安全管理的基本要求，包括网络数据安全管理要求、网络数据通用安全要求、网络数据处理活动安全要求和个人信息保护扩展要求。

本文件适用于指导各行业、各领域、各地区、各部门数据处理者开展网络数据安全管理工作，也可为数据安全监管部门、数据安全认证、评估、审计机构或其他有关组织对网络数据处理活动实施安全监管、评估提供参考。

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 35273—2020 信息安全技术 个人信息安全规范

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 data

任何以电子或者其他方式对信息的记录。

3.2

网络 network

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.3

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

3.4

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。

3.5

数据处理活动 data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等活动。

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］

3.6

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

［来源：GB/T 43697—2024，3.2］

3.7

核心数据 core data

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

［来源：GB/T 43697—2024，3.3］

3.8

一般数据 general data

核心数据、重要数据之外的其他数据。

［来源：GB/T 43697—2024，3.4］

3.9

个人信息 personal information

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

注 1：个人信息不包括匿名化处理后的信息。

注 2：个人信息包括姓名、出生日期、公民身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

［来源：GB/T 41479—2022，3.6］

3.10

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

［来源：GB/T 41479—2022，3.7］

3.11

个人信息主体 personal information subject

个人信息已识别或可识别（所标识或关联到）的自然人。

［来源：GB/T 41479—2022，3.8］

3.12

个人信息处理者 personal information processor

个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

3.13

数据合作方 data partner

通过业务合作、提供技术支撑和数据服务等，并可能接触到组织机构数据的外部机构。

3.14

第三方应用 third party application

由第三方提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务中的自动化工具。

注：本文件中的第三方应用包括但不限于软件开发工具包、第三方代码、组件、脚本、接口、算法模型、小程序等。

［来源：GB/T 41479—2022，3.12］

3.15

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

［来源：GB/T 41479—2022，3.13］

3.16

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

［来源：GB/T 35273—2020，3.15］

3.17

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019，3.12]

3.18

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。

注：根据发起者不同，分为自评估和检查评估。自评估由数据处理者自身发起，组成机构内部评估小组或委托第三方评估机构，依据有关政策法规与标准，对评估对象的数据安全风险进行评估的活动。检查评估由数据处理者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起的，依据有关政策法规与标准，对评估对象

的数据安全风险进行的评估活动。

3.19

大型互联网平台 large internet platform

通过网络技术将个人与个人、商品、信息、服务、线下资源、数据、资金、软件等进行连接，并以此为基础提供业务的较大规模的网络平台。

注 1：较大规模是指在过去的一年期间，在我国累计活跃用户总数不低于 5000 万。

注 2：提供业务包括但不限于即时通信、社交网络、电子商务、直播、短视频、信息资讯、应用商店、网络预约汽车、网络支付等。

4 网络数据安全管理总体框架

4.1 网络数据安全管理应包括网络数据安全管理要求、网络数据通用安全要求、网络数据处理活动安全要求和个人信息保护扩展要求四部分内容，网络数据安全管理要求指导落实网络数据处理活动安全要求和个人信息保护扩展要求，网络数据通用安全要求作为整体数据安全管理的基础技术支撑。其中，一般数据保护应满足数据安全的基本保护要求；重要数据保护应同时满足基本保护要求和重要数据扩展要求；核心数据应在重要数据保护的基础上依照有关规定从严保护；个人信息保护应在上述基础上，满足个人信息保护扩展要求。总体框架图见图 1。

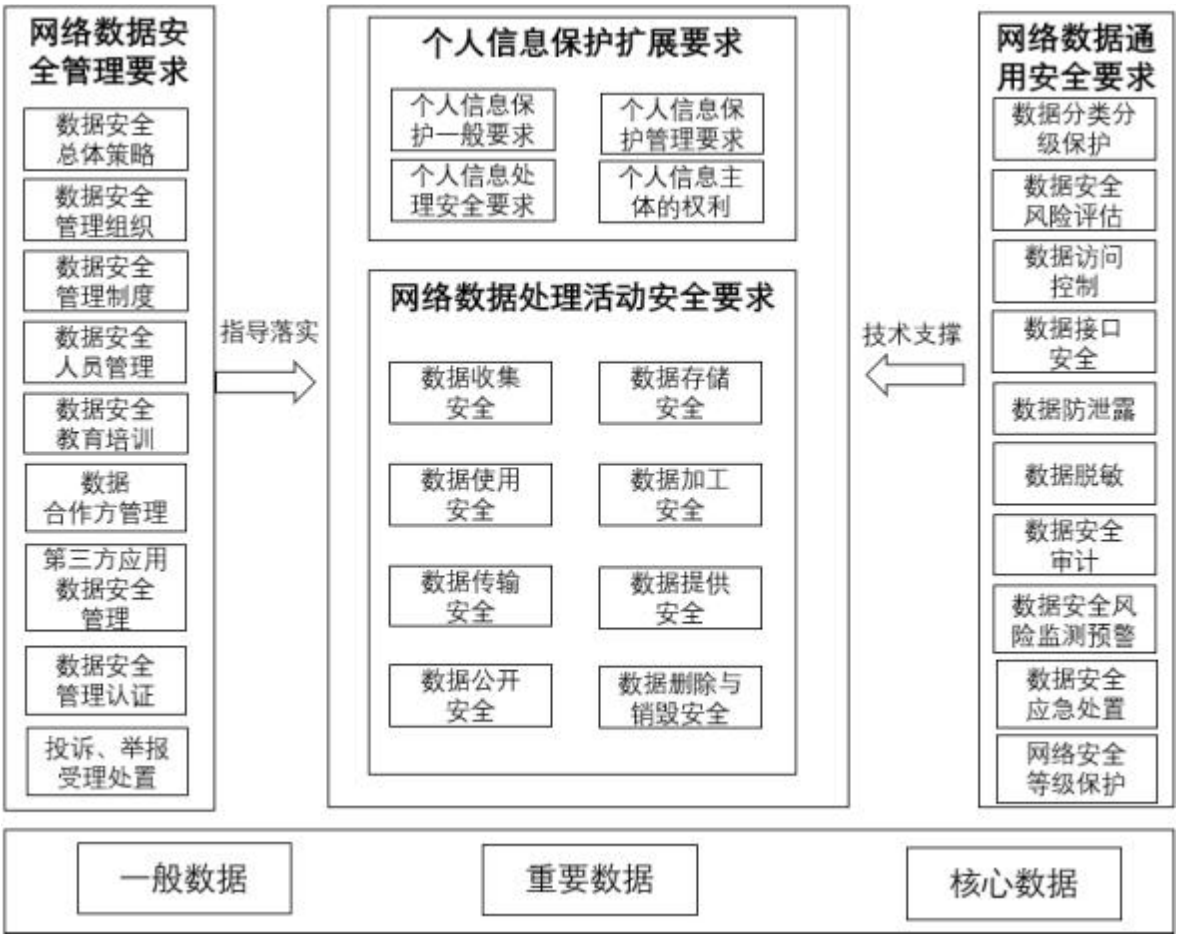
网络数据安全管理要求
数据安全总体策略
数据安全管理组织
数据安全管理制度
数据安全人员管理
数据安全教育培训
数据合作方管理
第三方应用数据安全管理
数据安全管理认证
投诉、举报受理处置
指导落实
个人信息保护扩展要求
个人信息保护一般要求
个人信息保护管理要求
个人信息处理安全要求
个人信息主体的权利
网络数据处理活动安全要求
数据收集安全
数据存储安全
数据使用安全
数据加工安全
数据传输安全
数据提供安全
数据公开安全
数据删除与销毁安全
技术支撑
网络数据通用安全要求
数据分类分级保护
数据安全风险评估
数据访问控制
数据接口安全
数据防泄露
数据脱敏
数据安全审计
数据安全风险监测预警
数据安全应急处置
网络安全等级保护
一般数据
重要数据
核心数据

图 1　总体框架图

4.2 网络数据安全管理要求

围绕数据安全总体策略、数据安全管理组织、数据安全管理制度、数据安全人员管理、数据安全教育培训、数据合作方管理、第三方应用数据安全管理、数据安全管理认证和投诉、举报受理处置等方面，建立完善符合法律法规、相关标准规范的数据安全管理组织。

4.3 网络数据通用安全要求

围绕数据分类分级保护、数据安全风险评估、数据访问控制、数据接口安全、数据防泄露、数据脱敏、数据安全审计、数据安全风险监测预警、数据安全应急处置、网络安全等级保护等方面落实基础安全管理措施。

4.4 网络数据处理活动安全要求

围绕数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等数据处理活动，开展数据安全管理，落实技术保护措施。

4.5 个人信息保护扩展要求

围绕个人信息保护一般要求、个人信息保护管理要求、个人信息处理安全要求以及个人信息主体的权利等方面规范保护要求，落实个人信息保护措施。

5 网络数据安全管理要求

5.1 数据安全总体策略

5.1.1 基本保护要求

5.1.1.1 应制定总体安全管理框架，明确数据安全管理总体策略，包括管理目标、原则、要求等内容。

5.1.1.2 制定数据安全管理总体策略应以重要数据、个人信息为重点。

5.1.2 重要数据保护扩展要求

无重要数据保护扩展要求。

5.2 数据安全管理组织

5.2.1 基本保护要求

5.2.1.1 应通过正式文件或制度明确数据安全管理各级组织及相应职责。

5.2.1.2 应明确数据安全负责人。职责包括但不限于负责牵头制定数据安全管理制度、指导数据安全管理工作、协调各相关部门开展数据保护工作、组织内部数据安全教育培训工作、提出数据安全保护的对策建议、监督管理制度和措施的执行落实情况等。

5.2.1.3 应明确数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

a) 研究提出数据安全相关重大决策建议；

b） 制定实施数据安全保护计划和数据安全事件应急预案；

c） 开展数据安全风险监测，及时处置数据安全风险和事件；

d） 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；

e） 受理、处置数据安全投诉、举报；

f） 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

5.2.1.4　应明确数据安全管理部门，牵头承担单位整体数据安全管理工作，落实数据安全保护责任。包括但不限于组织制定数据安全管理制度并执行，落实数据安全技术防护措施，开展数据安全教育培训、数据安全评估、数据安全监测、数据安全事件应急处置等工作。

5.2.1.5　应明确岗位职责和能力要求，足额配备具备相应岗位能力的数据安全人员，负责具体落实数据安全管理工作。包括但不限于数据梳理、分类分级、安全评估、合规性检查、权限管理、安全审计、监测预警、应急处置和信息报送、教育培训等工作。数据管理员、数据安全管理员、数据安全审计员应专人专岗。

5.2.1.6　宜建立独立的数据安全审计机构，负责开展数据安全和个人信息保护监督审计工作，并向管理层直接汇报。

5.2.2　重要数据保护扩展要求

5.2.2.1　重要数据处理者的数据安全负责人应由数据处理者决策层成员承担，并具备数据安全专业知识和相关管理工作经历。

5.2.2.2　掌握国家网信部门或者有关主管部门规定的特定种类、规模的重要数据的，数据安全管理机构应独立设立。

5.3　数据安全管理制度

5.3.1　基本保护要求

5.3.1.1　应建立健全数据安全管理制度，并通过正式、有效的方式发布数据安全管理制度和实施版本控制，并严格执行。

5.3.1.2　应形成由总体策略、管理规范、操作规程、记录表单等构成的数据安全管理制度体系。

5.3.1.3　制度体系内容应包括但不限于数据安全总体策略、组织机构与人员管理、数据分类分级、数据处理活动安全管理要求、数据访问控制、数据安全评估、数据安全审计、数据安全风险监测预警、数数据安全应急与处置、数据安全教育培训、合作方管理、数据出境、投诉举报受理处置等制度。

5.3.1.4　应建立数据安全制度文件管理控制流程，规范制度文件的建立、审批、发布、修订和废止，实施文件版本控制，确保制度文件的及时更新和有效访问。

5.3.1.5　应定期对数据安全管理制度的合理性、充分性和适用性进行论证和评价，对存在不足或需要改进的数据安全管理制度进行修订。

5.3.2　重要数据保护扩展要求

重要数据处理者应确保重要数据安全管理制度覆盖全部重要数据处理活动，并在安全环境、法规政策、组织架构或业务发生重大变化时及时评估和修订数据安全管理制度和安全策略。

5.4　数据安全人员管理

5.4.1　基本保护要求

5.4.1.1　应明确规定人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的数据安全管理要求并予以落实。

5.4.1.2　应明确人员岗位职责、数据访问和操作权限管理要求、人员调离保密要求、保密期限、违约责任等，定期审查其行为，对其数据操作行为进行有效约束。

5.4.1.3　在开展与关键信息基础设施网络安全和信息化有关的决策时，应有专门数据安全管理机构人员参与。

5.4.1.4　数据安全人员履职情况应留存相关工作记录，如数据安全管理监督检查记录、数据安全事件信息报送记录等。

5.4.2　重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据等人员落实资格审查、签署保密协议、审批和登记，明确岗位职责、数据访问范围、操作权限、人员调离保密要求、保密期限、违约责任等措施，定期审查其行为，对其数据操作行为进行有效约束。

5.5　数据安全教育培训

5.5.1　基本保护要求

5.5.1.1　应建立数据安全教育培训制度，明确培训周期、培训对象、培训内容、次数、课时和考核评价等。

5.5.1.2　应制定数据安全培训计划，定期（至少每年一次）或者政策发生变化时组织数据安全专业化培训工作，并对培训结果进行考核评价，留存相关记录（如培训计划、培训通知、培训课件、签到表、培训考核情况等相关记录文件）。

5.5.1.3　数据安全教育培训应覆盖单位全员，培训内容覆盖数据安全法律法规、单位制度要求和实操规范等内容。针对单位全员的培训内容包括但不限于普及数据安全意识、法律法规等，针对数据安全人员的培训内容包括但不限于标准规范、技能培训、安全评估、应急响应、应急演练等。

5.5.1.4　数据安全人员宜考取资质证书，持证上岗。

5.5.2　重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据的相关人员每年开展数据安全培训考核，依据考核结果确定任职资格。

5.6　数据合作方管理

5.6.1　基本保护要求

5.6.1.1　应明确管理相关数据合作方的数据安全管理部门和执行配合部门，并设置专岗负责相关工作，明确工作职责。

5.6.1.2　应梳理形成数据合作方清单并定期更新，合作方清单包含合作方名称、合作业务或系统、合作形式、合作期限、合作方联系人、合作涉及数据类型、数量以及数据重要程度等信息。

5.6.1.3　应建立数据合作方安全管理机制，如对合作方的选择、评价、管理、监督机制等。明确合作方的数据安全保护方式和责任落实要求，包括但不限于服务合同、合作方资质审核、接入管理、权限管理、主体授权、多个合作方管理、安全技术要求、数据脱敏、行为监测、数据销毁、数据安全应急响应及处置等管理要求。

5.6.1.4　应审核数据合作方的资质、网络和数据安全保障能力、业务连续性保障能力、数据安全事件

发生、数据安全事件应急响应和处置能力等情况，并开展安全评估。

5.6.1.5　应通过服务合同或安全保密协议等形式明确数据合作方的数据安全保护责任和义务。明确具体条款，包含但不限于下述内容：合作方及参与人员可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围、期限及用途（应符合最小化原则），合作方及参与人员的数据安全责任，合作方的保障措施配备情况（保障措施不低于本方的安全要求），合作结束后数据删除要求，合作方违约责任和处罚等。