ICS 35.030
CCS L 70

T/CSAS

团 体 标 准

T/CSAS 0020—2025

数据开发利用安全要求

Security requirements for data exploitation and utilization

2025-11-28 发布 2025-12-29 实施

四川省网络空间安全协会 发 布

目　　次

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。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：四川易利数字城市科技有限公司、全域数据信息安全重点联合实验室西南实验室、温州理工学院。

本文件主要起草人：曾凡、孔维、徐锴、赖一阳、田茂呈、刘明哲、项明荣（排名不分先后）。

引　言

随着信息技术的飞速发展和数据量的不断增长，数据已成为国家、企业乃至个人最重要的资产之一，数据开发利用也成了推动经济社会发展的重要力量。然而，数据在开发利用过程中，面临着诸多安全风险，如数据泄露、非法获取、篡改等，这些风险不仅可能导致巨大的经济损失，还可能对国家安全、社会稳定产生严重影响。正是由于数据安全问题的存在，政府、企业和个人对数据开发利用持谨慎态度，限制了数据要素市场化配置改革的进程。因此，制定《数据开发利用安全要求》团体标准，对于规范数据开发利用行为，保障数据安全，促进数据产业健康发展具有重要意义。本文件依从T/CSAS 0001—2025《数据生命周期安全参考框架》在数据采集、存储、加工、使用、归档以及销毁等全生命周期的安全管理要求。

数据开发利用安全要求

1 范围

本文件规定了数据开发利用的管理体系、技术要求、操作流程、风险评估与应对、培训与教育等方面的要求。

本文件适用于各类组织在非涉密数据开发利用过程中的安全管理，包括但不限于政府机构、企事业单位、社会团体等，涉密数据的开发利用在满足涉密要求的前提下，可参考本标准进行安全管理。

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 20984—2022 信息安全技术 信息安全风险评估方法
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 25062—2010 信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范
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
GB/T 37932—2024 信息安全技术 数据交易服务安全要求
GB/T 37964—2019 信息安全技术 个人信息去标识化指南
GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
GB/T 42250—2022 信息安全技术 网络安全专用产品安全技术要求
GB/T 42572—2023 信息安全技术 可信执行环境服务规范
GB/T 43580—2023 区块链和分布式记账技术 存证通用技术指南
GB/T 43697—2024 数据安全技术 数据分类分级规则
GB/T 44109—2024 信息技术 大数据 数据治理实施指南
T/CSAS 0001—2025 数据生命周期安全参考框架

3 术语和定义

GB/T 22239—2019、GB/T 25069—2022、GB/T 35273—2020、GB/T 37932—2019界定的以及下列术语和定义适用于本文件。

3.1

数据安全能力 data security capability

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

[来源：GB/T 37988—2019，3.5]

3.2

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识别的自然人有关的各种信息。

[来源：GB/T 43697—2024，3.5]

3.3

组织数据 organization data

组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据。

[来源：GB/T 43697—2024，3.9]

3.4

公共数据　public data

各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据。

[来源：GB/T 43697—2024，3.8]

3.5

可信存储　trust storage

通过密码技术、访问控制、日志审计等技术手段及管理机制，确保数据存储过程中具备机密性（如SM4 加密）、完整性（如SM3 哈希校验）、可追溯性（操作日志不可篡改）及可用性的存储体系。

注：相关技术要求可参考GB/T 42572—2023中关于存储可信性的要求。

4　基本原则

数据开发利用安全要求的总体原则如下：

a) 合法合规原则：数据开发利用相关方在各数据业务阶段中，应遵守法律法规等有关规定，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，不得危害国家安全、公共利益，不得损害个人、组织的合法权益；

b) 权责明确原则：应采取技术和其他必要的措施保障数据开发利用各业务阶段和数据处理环节的安全，对数据处理活动及数据要素流通活动中涉及的组织和个人的合法权益负责；

c) 最少必要性原则：数据开发利用活动仅处理满足特定公共服务所需的最少数据类型和数量；

d) 全程可控原则：数据开发利用各业务阶段包含数据交易过程，应确保数据来源合法可确认、使用范围可界定、交易过程可追溯、安全风险可防范、记录内容清晰，以防止数据被未授权访问、破坏、篡改、泄露或丢失等；

e) 分类分级原则：数据开发利用各活动交易标的应遵守国家和行业数据分类分级保护要求，结合数据流通范围、影响程度、潜在风险，建立公共数据、企业数据、个人信息等数据分类分级授权使用和保护机制；

f) 确保安全原则：数据开发利用相关方应采取必要的管理措施和技术手段，防范交易对象被篡改、破坏、泄露或者非法获取、非法利用、非法交易等风险，保障个人信息主体权益；

g) 明示同意原则：数据相关主体拥有对其个人信息的处理目的、方式、范围等规则的知情权，在进行数据处理活动前应向数据相关主体明示，并获得授权同意，法律、行政法规另有规定的例外情况，从其规定；

h) 目的明确原则：应制定数据开发利用安全防护策略，明确数据业务各阶段的安全防护目标和要求；

i) 动态调整原则：数据开发利用过程中的安全控制策略和安全防护措施应随着业务需求、安全环境属性、系统用户行为等因素进行动态调整。

5　数据开发利用安全总体框架

5.1　框架概述

依据《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》、GB/T 37988—2019以及数据开发利用的业务阶段，对数据开发管理内容、数据开发管理要素、数据开发利用业务阶段三个方面设计安全管理总体框架，如图1所示：

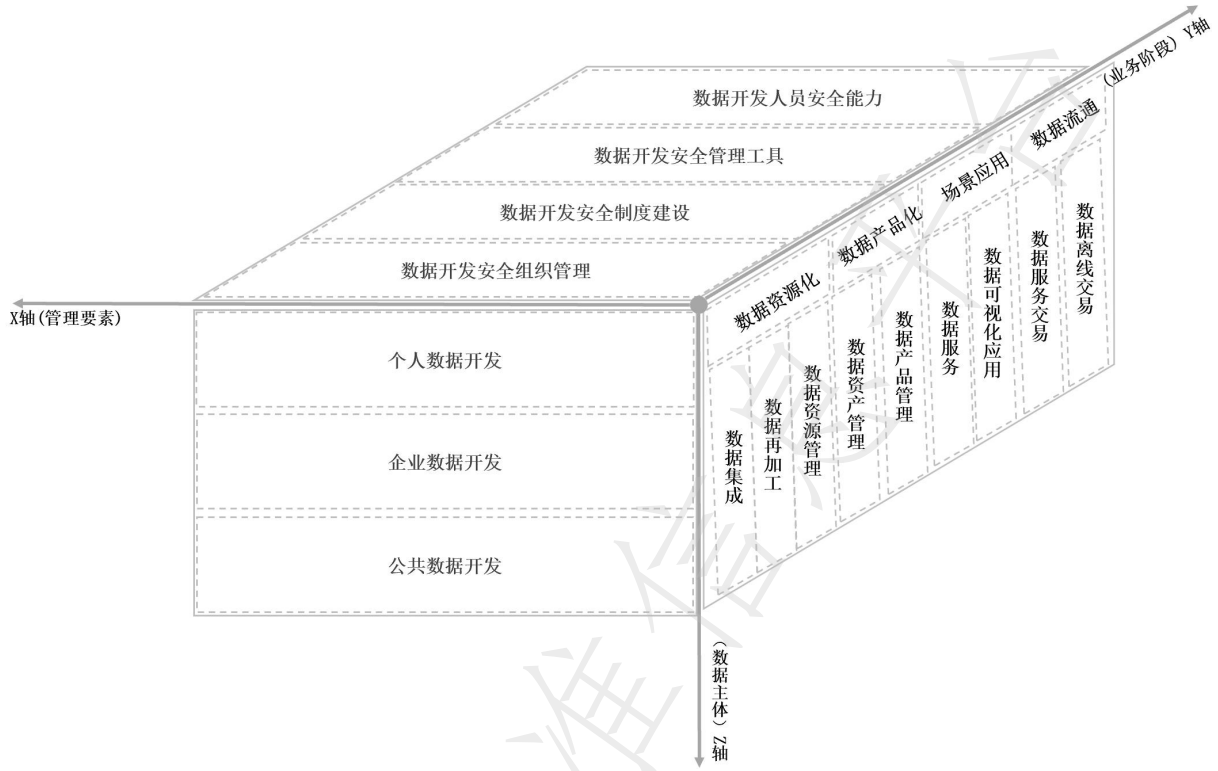

图 1　数据开发利用安全总体框架

5.2　数据开发利用业务阶段

数据要素作为第五生产要素，通过市场化产生价值。本框架中，以数据要素市场化维度为基础，融合数据开发生命周期，将数据开发利用划分为以下四个阶段：

a）　数据资源化阶段：主要包括数据集成、数据再加工、数据资源管理。其核心是解决数据从原始到可用，通过数据集成、清洗、加工等操作，将原始数据转化为结构化、可复用、可管理的数据资源，形成组织内部统一的数据资源池。阶段性标志为建立数据资源目录，将数据存入数据库，并实现资源级访问控制；

b）　数据产品化阶段：主要包括数据资产管理、数据产品管理。其核心是从可用到可交易，该阶段基于数据资源，通过权属确认、价值评估、封装加工，形成具备明确交易属性、可直接服务于市场需求的标准化数据产品。阶段性标志为明确定义产品权属与定价机制，通过产品形态封装，并通过合规性安全评估；

c）　场景应用阶段：主要包括数据服务、数据可视化应用。关键是“价值释放”，该阶段将数据资源或数据产品嵌入具体业务场景，通过服务化接口或可视化应用，直接支撑内部决策或对外提供服务。阶段性标志为通过最小化权限与动态脱敏控制实现与业务系统的集成，提供场景化数据服务/可视化输出；

d）　数据流通阶段：主要包括数据在线服务交易、数据离线交易。重点是“市场化”，该阶段中，数据产品通过交易平台或协议，以货币/等价物交换使用权的市场化流通行为，包含在线服务与离线交付两种形态。阶段性标志为通过交易所或第三方合规审核，实现全流程存证与溯源，并完成交易合约签署（含用途、期限限制）。

5.3　数据开发利用主体

数据主体参考GB/T 43697—2024，数据类型可依据不同的规则划分，本框架中主要从数据主体维度对数据开发管理的内容进行区分，分为个人数据开发、企业数据开发和公共数据开发。

5.4 数据开发管理要素

本框架依据GB/T 37988—2019，根据不同数据开发利用阶段以及不同数据主体将数据开发利用的安全性要求从四个安全能力维度（组织管理、制度建设、技术工具、人员能力）进行描述。

5.5 总体框架安全逻辑

本框架逻辑如下：

a) *X* 轴（管理要素），提供安全能力支撑，通过安全管理四要素落地具体安全要求。其中组织管理功能定位是明确责任主体与协作流程（比如明确责任部门），制度建设功能定位是制定规则与审批机制（比如数据分级、分类制度），管理工具功能定位在自动化防护与监控（比如加密模块、动态脱敏引擎），人员安全能力功能定位在保障执行专业性（比如安全操作培训）；

b) *Y* 轴（业务阶段），决定安全重点，根据数据价值转化流程，划分差异化的安全焦点。其中数据资源化的安全重点在于来源合规与质量可信，典型措施如分级分类、元数据追溯。数据产品化安全重点在于权属明确与封装安全，典型安全措施如资产确权。场景应用的安全重点在于最小化权限与动态控制，典型措施如实时脱敏。数据流通的安全重点在于全链路可追溯与风险隔离，典型措施如区块链存证与隐私计算交付；

c) *Z* 轴（数据主体）：决定安全底线，基于数据类型的内在属性，明确安全保护的核心目标与合规底线。其中个人数据以隐私保护为核心，遵循最小必要、明示同意原则。企业数据以商业秘密保护为基础，平衡经济价值与安全投入。公共数据以公共利益为重心，防范国家安全与社会秩序风险。

示例：个人数据在场景应用阶段的安全管控结合逻辑：

a) *Z* 轴底线约束（个人数据→隐私保护），要求可视化结果聚合展示（如用年龄区间代替出生日期）；

b) *Y* 轴阶段重点（场景应用→动态控制），实施字段级权限管理（如限制健康数据仅对医疗团队开放）；

C) *X* 轴能力支撑过程中，其中技术工具可嵌入实时脱敏引擎（例：调用 API 时自动掩码身份证号），制度建设可制定《数据展示最小化原则实施细则》，人员能力可要求运营人员需通过 CISP-PIP 认证。

5.6 关系说明

本文件第6章与第7章是第5章数据开发利用安全总体框架的具体安全要求：

第6章（一般性安全要求）主要聚焦 *X* 轴（管理要素）的横向能力支撑，覆盖全业务阶段共性的管理流程、技术措施及人员要求。

第7章（业务阶段安全要求）主要聚焦 *Y* 轴（业务阶段）的纵向场景深化，针对数据资源化、产品化、场景应用、流通四阶段细化差异化管理规范。

第6章和第7章通过“通用能力+场景适配”双维度协同，实现三维框架（数据主体×业务阶段×管理要素）的完整覆盖。

6 数据开发利用一般性安全要求

6.1 定位与框架性说明

本章规定数据开发利用全流程的共性安全要求，涵盖数据开发利用安全管控主要环节以及数据开发利用生命周期主要技术场景，并从安全四要素提出具体的共性安全要求，避免重复赘述。

数据开发利用安全管控依据ISO 27001的PDCA循环模型，通过顶层设计、保护基准、责任落地、动态防控、损失控制、闭环验证构建安全治理闭环，主要环节包括：安全策略规划（顶层设计）、数据分级分类（保护基准）、组织和人员管理（责任落地）、风险评估与应对（动态防控）、安全事件及应急处理（损失控制）以及监督与审计（闭环验证）。

数据开发利用生命周期主要技术场景依据T/CSAS 0001—2025，提取主要技术场景，具体包括数据传输、数据加密和解密、数据脱敏、鉴别与访问控制、数据存储、终端数据、网络可用性、数据销毁与留存。

6.2 数据开发利用安全管理流程

数据开发利用总体应遵循如图2所示的流程：

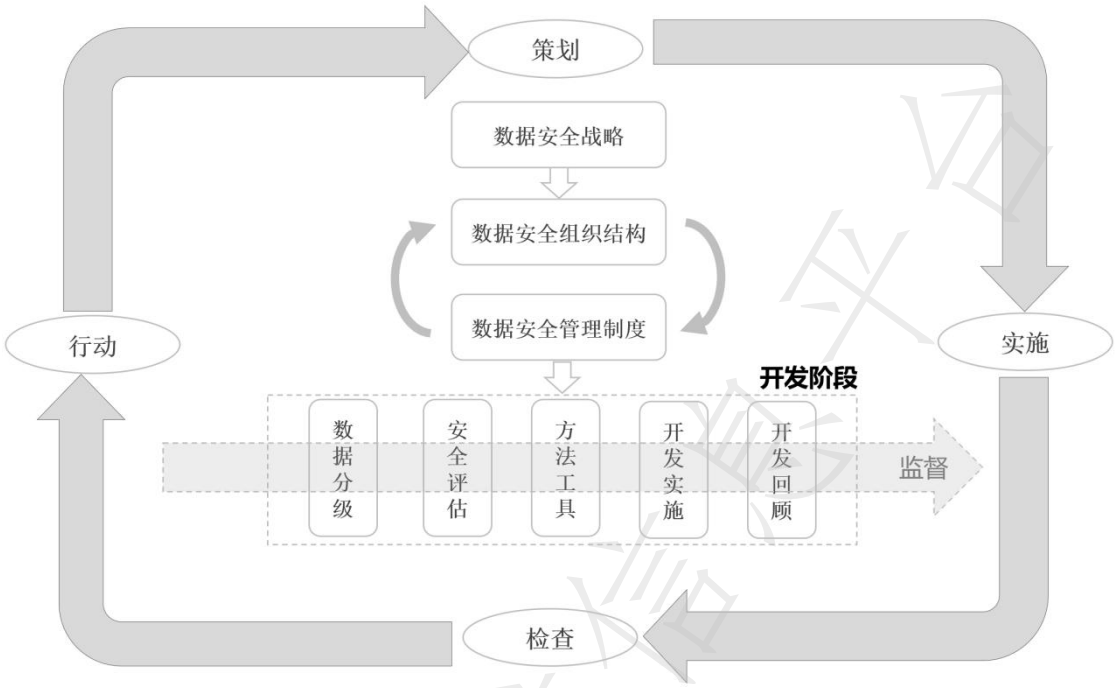

图 2　数据开发利用过程

组织应基于自身情况制定数据安全战略，依据数据安全战略成立相应组织并进行数据安全制度编制，进而倒逼组织结构优化。数据安全管理制度成熟后，在数据开发利用的业务阶段对数据进行分类分级、安全风险评估、确定方法和工具，组织开发实施，完成后进行回顾。

数据开发利用过程并不是一成不变，应按照过程改进的思想进行循环优化。

6.3　数据开发利用安全过程管控一般性要求

6.3.1　安全策略规划

安全策略规划是贯穿始终的“顶层设计”与“行动指南”，通过明确“安全目标、责任边界、管控规则、迭代机制”，将分散的安全措施（如终端防护、访问控制、存储加密等）整合为协同有效的体系，具体要求如下：

a)　组织结构要求：组织应设立专职的岗位和人员，负责组织数据安全制度流程和战略规划的建设；

b)　制度要求：

1)　应明确符合组织数据战略规划的数据安全总体策略，明确安全方针、安全目标和安全原则；

2)　应基于组织的数据安全总体策略，在组织层面明确以数据为核心的数据安全制度和规程，覆盖数据生存周期相关的业务、系统和应用，内容包含目的、范围、岗位、责任、管理层承诺、内外部协调机制及合规目标等；

3)　应明确并实施大数据系统和数据应用安全实施细则；

4)　应明确对数据资源生产、加工、使用、产品经营过程中的监督和管理细则；

5)　应明确运营机构的数据安全主体责任，以及需采取的必要安全措施，包括但不限于：每年修订 1 次数据安全总体策略；每季度组织 1 次跨部门安全协调会议；建立“策略－制度 －细则”三级文件体系，明确各岗位安全职责；

6)　应明确数据安全制度规程分发机制，将数据安全策略、制度和规程分发至组织相关部门岗位和人员；

7)　应明确数据安全制度及规程的评审、发布流程，并确定适当的频率和时机对制度和规程进行审核和更新；

8)　应明确组织层面的数据安全战略规划，包括各阶段目标、任务、工作重点，并保障其与业务规划相适应。

c)　安全开发工具要求：应建立数据安全策略规划系统，通过该系统向组织全体员工发布策略规划

的解读材料，以便于策略规划的落地推进；

d) 开发人员能力要求：

1) 负责制定数据安全总体策略和战略规划的人员应了解组织的业务发展目标，能将数据安全工作的目标和业务发展的目标进行有机结合；
2) 负责制定数据安全制度和规程的人员应具备信息安全管理体系建设的知识，并具备规范撰写能力；
3) 负责推广数据安全策略规划的人员应能以员工和相关方易理解的方式，通过培训等宣导形式对数据安全管理的方针、策略和制度进行有效传达。

6.3.2 数据分级分类

数据分级分类是数据安全与管理的基础性工作，是建立安全基准、精准防控数据安全风险的关键环节，具体要求如下：

a) 组织结构要求：组织应设立专职或兼职的岗位或人员负责数据安全分类分级工作；

b) 制度要求：

1) 应参考附录 A 数据分类分级原则、影响程度制定数据分类的方法和操作指南；
2) 应对组织的数据进行分类分级标识和管理；
3) 应对不同类别和级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施；
4) 应明确数据分类分级变更审批流程和机制，保证对数据分类分级的变更操作及其结果符合组织的要求。

c) 安全开发工具要求：应建立数据分类分级打标或数据资产管理工具，实现对数据的分类分级自动标识、标识结果发布、审核等功能；

d) 开发人员能力要求：负责该项工作的人员应了解数据分类分级的合规要求，能识别数据所属类别、级别。

6.3.3 组织和人员管理

组织和人员管理，是责任落地在安全过程管控中的重要环节，具体要求如下：

a) 组织结构要求：

1) 应建立组织层面的数据安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长的责任与权力；
2) 应建立组织层面专职的数据安全职能部门和岗位，并在职能岗位设计时考虑职责分离的原则；
3) 应建立组织内部的监督管理职能部门，负责对组织内部的数据操作行为进行安全监督；
4) 应明确在组织层面人力资源管理中承担数据安全要求制定和执行的人员或岗位，并与数据安全人员进行有效配合；
5) 应明确组织层面承担人员数据安全培训管理职责的岗位和人员，负责对数据安全培训需求的分析及落地方案的制定和推进；
6) 中小型组织可由“信息技术部门兼职承担数据安全管理职责”，无需设立专职部门。

b) 制度要求：

1) 应明确数据安全部门或岗位的要求，明确其工作职责、职能部门之间的协作关系和配合机制；
2) 应明确数据安全追责机制，定期对责任部门和安全岗位组织安全检查，形成检查报告；
3) 应明确数据服务人力资源安全策略，明确不同岗位人员在数据生存周期各阶段相关的工作范畴和安全管控措施；
4) 应明确组织层面的数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度，将数据安全相关的要求固化到人力资源管理流程中；
5) 应明确数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；
6) 应明确针对合作方的安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查；
7) 在重要岗位人员调离或终止劳动合同前，应与其签订保密协议或竞业协议；
8) 应明确组织内部员工的数据安全培训计划，按计划定期对员工开展数据安全培训，并在重要岗位转岗、岗位升级等环节对相关人员开展培训。

c） 安全开发工具要求：
1） 技术工具应实现数据安全相关的人力资源管理的自动化流程；
2） 应支持最少够用原则分配初始权限；
3） 应及时变更转岗员工的数据操作权限，并及时将人员的变更通知相关方；
4） 应以公开且可查询的形式，面向组织全员公布数据安全职能部门的组织架构；
5） 中小型组织推荐选用轻量化安全工具（如开源脱敏工具、云原生访问控制组件），降低成本。
d） 开发人员能力要求：
1） 负责组织和人员管理的人员应充分理解人力资源管理流程中可对安全风险进行把控的环节；
2） 负责设置数据安全职能的人员应能明确组织的数据安全工作目标。

6.3.4 风险评估与应对

风险评估与应对是保障数据安全、实现“动态防控”的核心环节，其贯穿于数据全生命周期的风险防控、合规落地和价值释放全过程，具体要求如下：

a） 组织结构要求：
1） 应由数据安全部门及业务部门负责对数据资源和影响数据资源安全的威胁源、脆弱性、已有安全措施及影响程度进行定期识别；
2） 应由数据安全部门及业务部门参考 T/CSAS 0001—2025 以及 GB/T 20984—2022 对数据开发利用安全风险进行评价并分类分级；
3） 由数据安全部门及业务部门负责对安全风险制定应对措施、定期进行监测，对安全应对措施的实施效果进行评估。
b） 制度要求：
1） 应制定相应的标准和制度以明确数据资源识别的机制、方法以及频率，明确数据资源安全威胁源、脆弱性、安全措施及影响程度；
2） 应制定相应的标准和制度以明确组织数据安全风险的分类、分级以及评价的方法；
3） 应明确组织数据安全风险监测、实施安全风险管控措施效果监测的方法及频率；
4） 应定期对核心数据、重要数据安全策略、规范、制度和管控措施进行风险评估，并及时响应。
c） 安全开发工具要求：
1） 应有对数据资源安全进行管理的技术手段；
2） 应部署对安全管控措施（如安全风险监测、检查以及实施风险应对等）进行审核及监控的技术工具。
d） 开发人员能力要求：
1） 应熟悉数据资源安全的威胁源、脆弱性、已有安全措施、影响程度以及安全风险级别的评估方法；
2） 应熟悉数据资源安全风险应对措施制定以及实施安全风险应对措施的方法；
3） 应熟悉组织数据资源的安全风险状态，包含安全风险发生概率、安全风险应对措施、残余安全风险等信息。

6.3.5 安全事件及应急处置

安全事件及应急处置是保障数据安全的“最后一道防线”，是及时损失控制在安全管控的重要环节，具体要求如下：

a） 组织结构要求：组织应设立专职负责数据安全事件管理和应急响应的岗位和人员；
b） 制度要求：
1） 应明确数据安全事件管理和应急响应工作指南，定义数据安全事件类型，明确不同类别事件的处置流程和方法；
2） 应明确数据安全事件应急预案，定期开展应急演练活动；
3） 组织的数据安全事件应急响应机制，应符合国家有关主管部门的政策文件要求。
c） 安全开发工具要求：
1） 应建立统一的安全事件管理系统，对日志、流量等内容进行关联分析；
2） 安全事件管理系统应能基于分析的内容实现预警及自动化响应决策。

d) 开发人员能力要求：负责该项工作的人员应具备安全事件的判断能力，熟悉安全事件应急响应措施。

6.3.6 监督与审计

监督与审计是数据安全管控的闭环验证环节，是确保全流程合规、保障管理措施落地的“免疫系统”，具体要求如下：

a) 组织结构要求：
   1) 应设立对核心数据、重要数据进行监控的岗位和人员；
   2) 应设立负责对数据生存周期各阶段的数据访问和操作安全风险进行监控和审计的岗位和人员；
   3) 宜定期或在发生重大信息安全事件后，对个人信息保护、重要数据保护、数据跨境传输方面的制度流程进行审核和检验，并将审核检验结果提交组织最高数据安全管理机构审批。
b) 制度要求：
   1) 应明确对组织内部各类数据访问和操作的日志记录要求、安全监控要求和审计要求；
   2) 应记录数据操作事件，并制定数据安全风险行为识别和评估规则；
   3) 应制定核心数据、重要数据的监控制度，防范重要数据安全事件；
   4) 应定期对组织内部员工数据操作行为进行人工审计。
c) 安全开发工具要求：
   1) 应采用自动和人工审计相结合的方法或手段对数据的高风险操作进行监控；
   2) 应建立针对数据访问和操作的日志监控技术工具，实现对数据异常访问和操作的告警，高敏感数据以及特权账户对数据的访问和操作应纳入重点监控范围；
   3) 应部署必要的数据防泄露实时监控技术手段，对个人信息、重要数据等的外发行为进行监控与报告；
   4) 应采用技术工具对数据交换服务流量数据进行安全监控和分析。
d) 开发人员能力要求：应了解数据访问和操作涉及的数据范围，具备对安全风险的判断能力。

6.4 数据开发利用技术安全一般性要求

6.4.1 数据传输

数据传输是数据在不同主体、系统、存储介质或网络空间之间进行转移、传递或交换的过程，其安全要求如下：

a) 组织结构要求：应由业务团队相关人员负责对传输通道进行加密处理；
b) 制度要求：
   1) 应明确数据传输安全管理规范和数据传输安全要求（如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等），确定需要对数据传输加密的场景；
   2) 应明确对数据传输安全策略变更进行审核的技术方案。
c) 安全开发工具要求：
   1) 应对传输数据的完整性进行检测，并具备数据容错或恢复的技术手段；
   2) 应部署对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的技术工具；
   3) 每个传输链路上的节点都应部署独立密钥对和数字证书，以保证各节点身份鉴别的有效性；
   4) 应综合量化敏感数据加密和数据传输通道加密的实现效果和成本，定期审核并调整数据加密的实现方案；
   5) 组织应提供统一的数据加密模块供开发传输功能人员调用，根据不同数据类型和级别进行数据加密处理，保证组织内数据加密功能的统一性；
   6) 传输协议应符合 GB/T 42250—2022 中关于安全通信协议的规定，优先采用传输层安全性协议（Transport Layer Security）1.3 或国密安全套接层（State-Cryptography Secure Sockets Layer, SM SSL）协议。
d) 开发人员能力要求：
   1) 应了解常用的安全通道方案、身份鉴别和认证技术、主管部门推荐的数据加密算法，并基于具体的业务选择合适的数据传输安全管理方式；

2） 负责该项工作的人员应熟悉数据加密的算法，并能基于具体的业务选择合适的加密技术。

6.4.2 数据加密和解密

数据加密和解密通过“技术隔离”构建安全屏障，如减少传输链路窃听、存储介质被盗、未授权访问、内部恶意泄露等风险，具体要求如下：

a） 组织结构要求：
   1） 组织专职或兼职员工负责制定数据加密、解密的原则和方法，并提供相关技术能力；
   2） 在数据存储、传输、使用阶段，应评估数据加密和解密的必要性，以及确定该场景下适用的数据加解密规则及方法。

b） 制度要求：
   1） 应明确组织的数据加解密规范，明确数据加解密的规则、加解密方法和使用限制等；
   2） 应明确需要加解密处理的应用场景、加解密处理流程、涉及部门及人员的职责分工；
   3） 应制定加解密过程中密钥管理的相应制度；
   4） 应明确列出需要加解密的数据资源，给出不同分类分级数据的加解密处理流程。

c） 安全开发工具要求：
   1） 数据加解密工具应优先选用国家密码管理部门认证的加密算法，包括但不限于商用密码 2 号椭圆曲线公钥密码算法（Elliptic Curve Cryptography Algorithm 2,SM2）、商用密码 4 号分组密码算法（SM4 Block Cipher Algorithm,SM4）、商用密码 9 号标识密码算法（Identity-Based Cryptography Algorithm 9,SM9）等商密算法，并支持向后兼容，以确保算法强度满足安全需求。非国密算法仅允许在国际合作、境外业务等经组织安全评估确认的特定场景使用，且需满足 GB/T 42250—2022 中关于境外数据传输的安全要求。
   2） 数据加解密工具应根据数据敏感程度（如个人信息、重要数据、核心数据）实施差异化加密策略，高敏感数据需采用强加密措施；
   3） 密钥的生成、存储、分发、轮换、撤销和销毁需符合安全管理规范，避免密钥泄露；
   4） 应对数据加解密处理过程中相应的操作进行记录，以满足数据加解密处理安全审计要求。

d） 开发人员能力要求：
   1） 人员应熟悉常规的数据加解密技术，能分析数据加解密过程中存在的安全风险，基于数据加解密的具体场景保证业务和安全之间的需求平衡；
   2） 应具备对数据加解密技术方案进行定制化的能力，基于组织内部各级别的数据建立有效的数据加解密方案。

6.4.3 数据脱敏

数据脱敏是通过对敏感信息进行变形、替换或屏蔽，在保留数据可用性的同时消除敏感性的技术手段，是平衡数据开发利用与隐私保护矛盾的必要手段，具体要求如下：

a） 组织结构要求：
   1） 组织专职或兼职员工负责制定数据脱敏的原则和方法，并提供相关技术能力；
   2） 在数据权限的申请阶段，应评估使用真实数据的必要性，以及确定该场景下适用的数据脱敏规则及方法。

b） 制度要求：
   1） 应明确组织的数据脱敏规范、规则、脱敏方法和使用限制等；
   2） 应明确需要脱敏处理的应用场景、脱敏处理流程、涉及部门及人员的职责分工；
   3） 应明确列出需要脱敏的数据资源，给出不同分类分级数据的脱敏处理流程；
   4） 应明确脱敏数据治理要求，在评估方法等方面反映脱敏治理效果。

c） 安全开发工具要求：
   1） 应实现数据脱敏工具与数据权限管理的联动，以及数据使用前的静态脱敏，并面向不同数据类型制定不同的脱敏方案，可基于场景需求自定义脱敏规则；
   2） 脱敏工具应对数据脱敏处理过程中相应的操作进行记录，满足数据脱敏处理安全审计要求；
   3） 数据脱敏后应保留原始数据格式和特定属性，满足开发与测试需求；
   4） 应对数据脱敏处理过程中相应的操作进行记录，以满足数据脱敏处理安全审计要求；
   5） 应具备基于机器学习的敏感数据自动识别、数据分析算法安全设计等数据分析安全能力。

d) 开发人员能力要求：
   1) 开发人员应熟悉常规的数据脱敏技术，能分析数据脱敏过程中存在的安全风险，基于数据脱敏的具体场景保证业务和安全之间的需求平衡；
   2) 应具备对数据脱敏的技术方案进行定制化的能力，能基于组织内部各级别的数据建立有效的数据脱敏方案。

6.4.4 鉴别与访问控制

鉴别是确认用户/实体身份真实性的过程，访问控制是基于身份和权限限制数据操作范围的机制，二者共同构成数据安全的“第一道防线”，贯穿数据资源化、产品化、数据流通等各业务阶段，具体要求如下：

a) 组织结构要求：应负责制定组织内用户身份鉴别、访问控制和权限管理的策略，提供相关技术能力或进行统一管理；
b) 制度要求：
   1) 应明确组织的身份鉴别、访问控制与权限管理要求，明确对身份标识与鉴别、访问控制及权限的分配、变更、撤销等权限管理的要求；
   2) 应按最少够用、职权分离等原则，授予不同账户完成各自承担任务所需的最小权限，并在各账户之间形成相互制约关系；
   3) 应明确数据权限授权审批流程，对数据权限申请和变更进行审核；
   4) 应定期审核数据访问权限，及时删除或停用多余的、过期的账户和角色，避免共享账户和角色权限冲突的存在；
   5) 应对外包人员和实习生的数据访问权限进行严格控制；
   6) 应建立数据安全角色清单，明确数据安全角色的安全要求、分配策略、授权机制和权限范围。
c) 安全开发工具要求：
   1) 应建立组织统一的身份鉴别管理系统，支持组织主要应用接入，实现对人员访问数据资源的统一身份鉴别；
   2) 应建立组织统一的权限管理系统，支持主要应用接入，对人员访问数据资源进行访问控制和权限管理；
   3) 应采用技术手段实现身份鉴别和权限管理的联动控制；
   4) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术实现；
   5) 访问控制的粒度应达到主体为用户级，客体为系统、文件、数据库表级或字段；
   6) 应建立面向数据应用的访问控制机制，包括访问控制时效的管理和验证，以及数据应用接入的合法性和安全性取证机制；
   7) 应建立人力资源管理与身份鉴别管理、权限管理的联动机制，及时删除离岗、转岗人员的权限；
   8) 应采用技术手段对系统或应用访问敏感数据进行访问控制。
d) 开发人员能力要求：负责该项工作的人员应熟悉相关的数据访问控制技术知识，并能根据组织数据安全管理制度对数据权限进行审批管理。

6.4.5 数据存储

数据存储是数据全生命周期的“保险箱”，其安全直接决定数据在静态状态下的防护能力，具体安全要求如下：

a) 组织结构要求
   1) 应设立统一的数据存储安全管理岗位，明确整体的存储媒体以及逻辑存储系统安全管理要求，并推进相关要求的实施；
   2) 应明确各数据逻辑存储系统的安全管理员职责，负责执行存储设备、数据逻辑存储系统及媒体存储的安全管理和运维工作；
   3) 应设立统一数据备份和恢复的岗位和员工负责建立相应的制度并部署相关的安全措施。
b) 制度要求
   1) 应明确存储媒体访问和使用的安全管理规范，建立存储媒体使用的审批和记录流程；

2） 应建立存储媒体资产标识，明确存储媒体存储的数据；
3） 应对存储媒体进行常规和随机检查，确保存储媒体的使用符合组织存储媒体使用的制度；
4） 应明确数据逻辑存储管理安全规范和配置规则，明确各类数据存储系统的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的要求；
5） 应明确数据备份与恢复的管理制度，满足数据服务可靠性、可用性等安全目标；
6） 应明确数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志记录、数据保存时长等；
7） 应明确数据备份与恢复的定期检查和更新工作程序，包括数据副本的更新频率、保存期限等；
8） 应依据数据生存周期和业务规范，建立数据生存周期各阶段数据归档的操作流程；
9） 应明确数据存储时效性管理规程，明确数据分享、存储、使用和删除的有效期、有效期到期时对数据的处理流程、过期存储数据的安全管理要求。

c） 安全开发工具要求
1） 技术工具对存储媒体性能进行监控，包括存储媒体的使用历史、性能指标、错误或损坏情况，对超过安全值的存储媒体进行预警；
2） 应对存储媒体访问和使用行为进行记录和审计；
3） 应为数据存储系统配置扫描工具，定期对主要数据存储系统的安全配置进行扫描，以保证符合安全基线要求；
4） 应利用技术工具监测逻辑存储系统数据使用的规范性，确保数据存储符合组织的相关安全要求；
5） 可在个人信息、重要数据等数据有恢复需求时，采取必要的技术手段恢复数据；
6） 应建立数据备份与恢复的统一技术工具，保证相关工作的自动执行；
7） 应建立备份和归档数据安全的技术手段，包括但不限于对备份和归档数据的访问控制、压缩或加密管理、完整性和可用性管理，确保对备份和归档数据的安全性、存储空间的有效利用、安全存储和安全访问；
8） 应定期采取必要的技术措施查验备份和归档数据完整性和可用性；
9） 应建立过期存储数据及其备份数据的彻底删除或匿名化的方法和机制，能验证数据已被完全删除、无法恢复或个人信息无法识别，并告知数据控制者和数据使用者；
10） 应通过风险提示和技术手段避免非过期数据的误删除，确保在一定时间窗口内被误删的数据可以手动恢复；
11） 应确保存储架构具备数据存储跨机柜或跨机房容错部署能力。

d） 开发人员能力要求：
1） 应熟悉存储媒体安全管理的相关合规要求，熟悉不同存储媒体访问和使用的差异性；
2） 应熟悉数据存储系统架构，并能分析出数据存储面临的安全风险，从而保证对各类存储系统的有效安全防护；
3） 应了解数据备份媒体的性能和相关数据的业务特性，确定有效的数据备份和恢复机制；
4） 负责该项工作的人员应了解数据存储时效性相关的合规性要求，并具备基于业务对合规要求的解读能力和实施能力。

6.4.6 终端数据

终端是数据“产生、采集、访问、输出”的“神经末梢”，终端数据的安全状态直接影响数据从源头流转到各环节的安全性，对其安全要求如下：

a） 组织结构要求：组织内应设立统一的终端设备或办公数据安全管理岗位和人员；
b） 制度要求
1） 组织应明确面向终端设备的数据安全管理规范，明确终端设备的安全配置管理、使用终端数据的注意事项和数据防泄露管理要求等；
2） 组织应定期对终端数据防泄露解决方案的成效进行量化评估，评估新风险和需要调整的控制措施，量化提升组织整体的终端数据防泄露方案。

c） 安全开发工具要求：
1） 打印输出设备应采用身份鉴别、访问控制等手段进行安全管控，并对用户账户在此终端设

备上的数据操作进行日志记录；
2) 组织内入网的终端设备均应按统一的要求部署防护工具（如防病毒、硬盘加密、终端入侵检测等软件），并定期进行软件的更新，将终端设备纳入组织整体的访问控制体系中；
3) 应提供整体的终端安全解决方案，实现终端设备与组织内部员工的有效绑定，按统一的部署标准在终端设备系统上安装各类防控软件（如防病毒、硬盘加密、终端入侵检测等软件），并定期进行软件的更新，将终端设备纳入组织整体的访问控制体系中；
4) 终端数据安全自动化工具应能量化统计数据安全泄漏风险，并展示相关风险，为后续终端数据安全管控能力提升提供技术支持。

d) 开发人员能力要求：负责该项工作的人员应充分了解终端设备的数据出入口以及相应的数据安全风险，能利用相应的工具实现整体的安全控制方案。

6.4.7 网络可用性

网络可用性是保障数据“安全措施有效落地”的基础支撑，直接影响数据采集、传输、处理、共享等环节的安全性与有效性。具体安全要求如下：

a) 组织结构要求：应有专有或兼职人员针对网络可用性进行管理和维护；
b) 制度要求：应设立网络可用性关键指标，包括可用性的概率数值、故障时间、频率、统计业务单元等，并基于可用性管理指标，制定网络服务配置方案和宕机替代方案；
c) 安全开发工具要求：
1) 应通过相关指标定量分析网络可用性及数据防泄露服务现状，并有针对性地解决问题，提升网络可用性；
2) 应对关键的网络传输链路、网络设备节点实行冗余建设，并部署相关设备（如负载均衡、防入侵攻击、数据防泄露检测与防护等设备）对网络可用性及数据泄露风险进行防范。
d) 开发人员能力要求：负责网络资源管理的人员应具有网络安全管理的能力，了解网络安全中对可用性的安全需求，能根据不同业务对网络性能的需求制定有效可用的安全防护方案。

6.4.8 数据留存与销毁

数据留存与数据销毁是一对“逆向互补”的安全控制手段。数据留存聚焦“数据在合法、必要期限内的安全存储”，数据销毁关注“数据超出使用价值或期限后彻底消除风险”，两者共同构成数据“从产生到消亡”的闭环安全管理，具体安全要求如下：

a) 组织结构要求：应有专有或兼职的岗位负责数据的统一销毁，并制定数据销毁处置规范，推动相关要求的落地实施；
b) 制度要求：
1) 应按照数据分类分级建立数据销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式和销毁要求；
2) 应建立规范的数据销毁流程和审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录；
3) 应按照国家相关法律和标准销毁个人信息、重要数据等敏感数据。
c) 安全开发工具要求：
1) 应对网络存储数据，建立硬销毁和软销毁的数据销毁方法和技术，如基于安全策略、基于分布式杂凑算法等网络分布式存储销毁策略与机制；
2) 应配置必要的数据销毁技术手段与管控措施，确保以不可逆方式销毁敏感数据及其副本内容。
d) 开发人员能力要求：熟悉数据销毁工作的相关安全、合规要求。

7 数据开发利用业务阶段安全要求

7.1 定位与框架性说明

本节侧重介绍 *Y* 轴（业务阶段）在各个业务阶段的安全重点，在依从当前阶段共性安全要求的基础上，从安全管理四要素提出具有其业务特征的安全要求。

7.2 数据资源化管理过程

7.2.1 数据采集

7.2.1.1 数据采集组织管理

在数据集成阶段，对公共数据、个人数据以及企业数据的开发利用安全组织要求如下：

a) 组织应设立专职或兼职的岗位或人员负责如下工作：
   1) 制定相关数据采集安全管理制度，推动相关要求、流程的落地；
   2) 对数据资源的风险评估提供咨询和支持；
   3) 制定统一的数据质量管理要求，对数据质量进行管理和监控。
b) 可引入第三方机构、数据商协助对数据源的数据安全地采集。

7.2.1.2 数据采集制度建设

在数据采集阶段，数据（包含公共数据、个人信息以及企业数据）的开发利用安全制度要求如下：

a) 遵循 T/CSAS 0001—2025《数据生命周期安全参考框架》对数据采集的要求；
b) 应明确核心业务数据采集原则，定义业务的数据采集流程和方法；
c) 应明确数据采集的渠道及外部数据源，并对外部数据源的合法性进行确认；
d) 应明确数据采集范围、数量和频度，确保不收集与提供与服务无关的个人信息和重要数据；
e) 应明确组织数据采集的风险评估流程，针对采集的数据源、频度、渠道、方式、数据范围和类型进行风险评估；
f) 应定义数据追溯策略要求、追溯数据格式、追溯数据安全存储与使用的管理制度等；
g) 应梳理组织内的业务数据源类型，并明确在关键的数据管理系统（如数据库管理系统、元数据管理系统）上对数据源标记的要求；
h) 应制定引入第三方机构、数据商采集数据的安全管理制度要求；
i) 针对企业数据，还应制定商业秘密保护制度；
j) 针对个人信息，还应要求：
   1) 应明确数据采集过程中个人信息和重要数据的知悉范围和需要采取的控制措施，确保采集过程中的个人信息和重要数据不被泄露；
   2) 应基于国家针对个人数据采集的要求制定相关制度，包含但不限于如下要求：
      - 个人信息的收集、使用、加工、传输和提供必须基于合法、正当、必要的原则，只有在用户知情并明确同意的情况下才能进行；
      - 仅采集所必需的最少个人信息，并且尽可能采取去标识化或匿名化处理，降低数据泄露带来的风险；
      - 明确个人信息的公共属性部分，公共属性部分的个人信息采集仍需要获得用户的知情和明确同意的情况下才能进行；
      - 须严格遵守当地的个人信息保护、网络安全及数据安全方面的相关法律法规，如我国的《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等，以及欧盟《一般数据保护法案》（General Data Protection Regulation，GDPR）等数据保护条例；
      - 个人信息在用于公共卫生、公共安全等公共利益场景时，应遵循《中华人民共和国个人信息保护法》第十三条规定，确保处理范围与公共利益目的匹配，且不超出必要限度。

7.2.1.3 数据采集管理工具

在数据采集阶段对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a) 应依据统一的数据采集流程建设数据采集相关的工具，以保证组织数据采集流程实现的一致性，同时相关系统应具备详细的日志记录功能，确保数据采集授权过程的完整记录；
b) 应根据制度流程的更新，不断优化数据采集工具；
c) 针对个人信息开发利用的安全管理工具还应要求：
   1) 个人数据的隐私部分应该按照分级、分类的规则，将获得个人数据的标志性属性进行脱敏处理；

2) 个人数据公共属性部分的采集应提示用户哪些公共属性信息需要被采集，其用途是什么，用户授权后方能进行采集。

7.2.1.4 数据采集人员能力

在数据采集阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员应充分理解数据采集的法律要求、安全和业务需求，并能根据组织的业务提出针对性的解决方案。

针对个人信息开发利用的数据采集人员能力还应要求：参与个人数据采集的开发人员应了解个人信息的分级、分类，并熟悉个人数据采集的政策，合法、合规地采集数据。

7.2.2 数据再加工

7.2.2.1 数据再加工组织管理

在数据再加工阶段，对数据（包含公共数据、个人信息以及企业数据）的开发安全组织要求如下：

a) 组织应设立专职或兼职的岗位或人员负责以下的工作：
   1) 制定相关的数据加工安全管理及安全审计制度，推动相关要求、流程的落地；
   2) 对具体业务或项目的数据再加工风险评估提供咨询和支持；
   3) 编制数据再加工安全操作指南；
   4) 对负责具体数据加工的业务团队提供安全咨询；
   5) 监督检查或审计数据再加工的安全操作；
   6) 负责对数据正当使用管理、评估和风险控制；
   7) 负责数据处理环境安全管控；
   8) 负责制定数据导入导出规则和提供技术指导，在组织内推动业务落地执行。
b) 组织业务部门的业务团队安全要求如下：
   1) 负责数据采集和加工的安全管理；
   2) 负责对具体场景下的数据传输通道进行加密处理；
   3) 引入第三方机构或数据商协助进行数据的再加工。

7.2.2.2 数据再加工制度建设

在数据再加工阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全制度要求如下：

a) 应梳理组织内的业务数据源类型，并明确在关键的数据管理系统（如数据库管理系统、元数据管理系统）上对数据源进行标记的要求；
b) 应采取必要的监控审计措施，确保实际进行的数据再加工的安全技术和安全管理过程与计划保持一致，整体保证满足数据再处理安全要求；
c) 应制定数据再加工环境的系统设计、开发和运维阶段相应的安全控制措施，实现对安全风险的管理；
d) 组织应基于数据再加工环境建立分布式处理安全要求，对外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄露等方面进行安全要求和控制；
e) 应依据数据分类分级要求建立符合业务规则的数据导入导出安全策略，如授权策略、流程控制策略、不一致处理策略等；
f) 应明确数据输出安全评估和授权审批流程，评估数据输出的安全风险，并对大量或敏感数据输出进行授权审批；
g) 应建立针对数据再处理输出存储媒体的标识规范，明确存储媒体的命名规则、标识属性等重要信息，定期验证输出数据的完整性和可用性；
h) 应制定输入输出审计策略和日志管理规程，并保存导入导出过程中的出错数据处理记录；
i) 组织应制定引入第三方机构或数据商协助进行数据再加工的安全管理制度；
j) 在个人信息数据再加工过程中，安全制度可参考 7.2.1.2 的要求。

7.2.2.3 数据再加工管理工具

在数据再加工阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a） 应记录并保存数据处理与分析过程中对个人信息、重要数据等敏感数据的操作行为；
b） 应提供组织统一的数据再加工系统，并能呈现数据再加工前后数据间的映射关系；
c） 应在数据再加工过程中提供对数据脱敏的功能要求；
d） 应完整记录数据再加工过程的操作日志，以备对潜在违规再加工者责任的识别和追责；
e） 数据处理系统与数据权限管理系统联动，用户在使用数据处理系统前已获得授权；
f） 基于数据处理系统的多租户特性，保证不同租户在该系统中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制；
g） 应建立数据处理日志管理工具，记录用户在数据处理系统上的加工操作，提供数据在系统上加工计算的关联关系；
h） 对分布式处理过程中不同数据副本节点数据的完整性和一致性进行定期检测；
i） 应建立分布式处理节点和用户安全属性的周期性确认机制；
j） 应建立数据分布式处理节点的服务组件自动维护和管控措施，包括虚假节点监测、故障用户节点确认和自动修复的技术机制；
k） 应建立分布式处理外部服务组件注册与使用审核机制；
l） 应具备对密文数据进行搜索、排序、计算等透明处理的技术能力；
m） 应建立分布式处理过程中的数据泄露控制机制，防止数据处理过程中的调试信息、日志记录等不受控制输出导致受保护个人信息、重要数据等敏感数据的泄露；
n） 应记录并定期审计组织内部的数据导入导出行为，确保未超出数据授权使用范围；
o） 对数据输入输出终端设备、用户或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的保证；
p） 在导入导出完成后应对数据导入导出通道缓存的数据进行删除，以保证导入导出过程中涉及的数据不会被恢复；
q） 应采取多因素鉴别技术对数据导入导出操作人员进行身份鉴别；
r） 应为数据导入导出通道提供冗余备份能力；
s） 应对数据导入导出接口进行流量过载监控；
t） 应建立组织统一的数据导入导出管理系统，提示数据导入导出的安全风险并进行在线审核；
u） 应配置规范的数据导入导出机制或服务组件，明确数据导入导出最低安全防护要求；
v） 针对个人信息，还应具备数据主体权利响应系统，如数据主体访问请求（Data Subject Access Request, DSAR）的相关功能要求。

7.2.2.4 数据再加工人员能力

在数据再加工阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a） 应基于合规性要求，对数据再加工过程中所可能引发的数据聚合安全风险进行有效评估，并针对分析场景提出有效的解决方案；
b） 负责该项工作的人员应按最小够用原则管理权限，并具备对数据再加工相关风险的分析和跟进能力；
c） 负责数据再加工人员应具备发现数据再加工过程中安全风险的能力；
d） 负责该项工作的人员应了解数据环境下数据处理系统主要的安全风险，并能在相关的系统设计、开发阶段通过合理的设计以及运维阶段的有效配置规避相关风险；
e） 负责数据导入导出安全工作的人员应充分理解组织的数据导入导出规程，并根据数据导入导出的业务执行相应的风险评估，提出实际的解决方案；
f） 针对个人信息，开发人员还应了解个人信息的分级、分类，并熟悉个人数据再加工政策，合法、合规地再加工数据。

7.2.3 数据资源化管理

7.2.3.1 数据资源化组织管理

在数据资源管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发安全组织要求如下：

a） 组织应设立专职或兼职的岗位或人员负责以下工作：

1） 制定相关的数据资源安全管理制度，推动相关要求、流程的落地；
2） 对业务部门数据资源管理的风险评估提供咨询和支持；
3） 监督检查或审计数据资源的安全管理操作；
4） 负责统一管理数据开发资源的安全管理；
5） 制定引入第三方机构或数据商协助数据资源盘点和梳理的相关安全管理制度；

b） 组织业务部门的业务团队建立数据资源管理制度，对组织的数据资源进行鉴别和记录。

7.2.3.2 数据资源化制度建设

在数据资源阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全制度要求如下：

a） 数据资源的管理应覆盖整个数据资源化过程；
b） 应定义数据资源安全管理的相关制度，并包含对数据资源主体的安全管理制度；
c） 应梳理组织内的各类数据源及其类型，采用元数据描述数据资源并明确在数据资源管理系统上对数据资源进行记录的要求；
d） 应定义数据资源的源数据追溯策略要求、追溯数据格式、追溯数据安全使用的管理制度等；
e） 应定义数据资源的安全审计管理要求，包含审计的频度、次数、审计管理要求等；
f） 制定第三方机构或数据商协助数据资源盘点和梳理的相关安全管理制度；
g） 针对个人信息，应充分考虑个人数据的隐私部分，并按照分级、分类的规则进行资源管理。

7.2.3.3 数据资源化管理工具

在数据资源管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a） 应以元数据的形式描述组织所有的数据资源分类、名称、主体、数据源、数据处理方法，并进行记录和保存；
b） 应记录数据资源信息变动的日志信息，便于对数据资源的安全审计；
c） 应记录数据资源被访问提取的日志信息，便于对数据资源访问的安全审计和分析；
d） 应对所有数据资源进行打标并版本化管理；
e） 数据资源被访问时应参考一般性要求中的鉴别和访问机制进行管理；
f） 数据资源应参考一般性安全要求的分级、分类要求对数据资源进行分级、分类，并根据级别和类别的不同对数据资源进行可信存储（可信存储可以是组织内部经过鉴定的区块链、数据仓库、数据库、磁阵等其它可存储的设备设施，也可以是外部组织经过权威部门鉴定过的区块链、数据仓库、数据库等可存储的设备、设施）；
g） 应提供组织对数据资源安全管理的统计图表，包含对数据资源存储状态、数据资源访问情况、数据资源变化情况等的统计分析；
h） 应利用机器学习对数据资源的安全管理情况进行识别和分析，并作出预警。

7.2.3.4 数据资源化人员能力

在数据资源管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a） 应熟悉数据资源安全管理的制度、流程，并基于制度、流程对数据资源进行安全管理；
b） 应能基于安全管理工具的信息对数据资源的安全性进行判断和分析；
c） 数据资源的安全审计人员应能基于制度对数据资源的安全管理合规性进行审计；
d） 针对个人信息，还应要求参与个人数据资源管理的开发人员了解个人信息的分级、分类，并熟悉个人数据资源管理的政策，合法、合规地管理个人数据资源。

7.3 数据产品化管理过程

7.3.1 数据资产化管理

7.3.1.1 数据资产化组织管理

在数据资产化阶段，对数据（包含公共数据、个人信息以及企业数据）的开发安全组织要求如下：

a） 组织应设立专职或兼职的岗位或人员负责以下工作：

1） 制定相关的数据资产化安全管理（如确权、评估等）制度，推动相关要求、流程的落地；
2） 对业务部门数据资产化管理的风险评估提供咨询和支持；
3） 监督检查或审计数据资产化的安全管理操作；
4） 负责统一管理数据资产化的安全管理；
5） 制定引入第三方机构或数据商协助数据资产化的相关安全管理制度。

b） 针对公共数据的组织安全管理还应要求：
1） 设立公共数据安全管理组织，统筹协调数据开放共享与安全风险管控；
2） 明确公共数据资产化责任主体，由数据提供组织与使用组织联合签署安全协议。

c） 针对企业数据的组织安全管理，还应要求建立跨部门数据安全协作机制，业务部门与技术部门联合制定资产化方案；

d） 针对个人信息的组织安全管理，还应要求建立独立的数据合规审计团队，定期评估匿名化、去标识化效果。

7.3.1.2 数据资产化制度建设

在数据资产化阶段，对数据资产（包含公共数据、个人信息以及企业数据）的开发利用安全制度要求如下：

a） 应定义数据资产安全管理（如确权、评估等）相关制度，并包含对数据资产主体的安全管理制度；

b） 应梳理组织内的各类数据资产及其类型，采用元数据描述数据资产并明确在数据资产管理系统上对数据资产进行记录的要求；

c） 应定义数据资产确权、评估的安全审计管理要求，包含审计的频度、次数、审计管理要求等；

d） 针对公共数据，还应要求：
1） 明确敏感数据（如地理、人口等）的资产化审批流程；
2） 制定数据共享负面清单，禁止涉及国家安全、公共利益的原始数据直接资产化。

e） 针对企业数据的安全制度还应要求：
1） 制定商业秘密数据资产化白名单，禁止核心工艺、客户清单等数据直接交易；
2） 建立数据资产化收益分配制度，明确数据贡献方、加工方、使用方的权利与责任。

f） 针对个人信息的安全制度还应要求：
1） 遵循“知情—同意”原则，在隐私政策中明示数据资产化的目的与范围；
2） 建立个人信息主体权利响应机制，支持查询、更正、删除资产化数据。

7.3.1.3 数据资产化管理工具

在数据资源管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a） 应以元数据形式描述组织所有数据资产的分类、名称、主体、数据源、数据处理方法，并记录和保存；

b） 应记录数据资产信息变动的日志信息、数据资产被访问提取的日志信息，便于对数据资产化过程的安全审计；

c） 应对所有数据资产进行打标并版本化管理；

d） 数据资产（如实体化数据资产、权益性成果等）应参考 7.2.3.3 进行分级分类存储；

e） 可提供组织对数据资产安全管理的统计图表，包含对数据资产存储状态、数据资产访问情况、数据资产变化情况等的统计分析；

f） 应利用机器学习对数据资产的安全管理情况进行识别和分析，并作出预警；

g） 针对公共数据的开发管理工具还应要求：
1） 采用数据脱敏、差分隐私技术处理公共数据，确保资产化后无法逆向识别个体或实体；
2） 应部署数据流转监测工具，记录公共数据资产化过程中的访问、加工、输出行为。

h） 针对企业数据的开发管理工具还应要求：
1） 应部署数据溯源追踪工具，记录企业数据在资产化过程中的加工路径与权限变更；
2） 应对高价值数据（如商业洞察报告）采用数字水印技术，防止非法泄露与滥用。

i） 针对个人信息的开发管理工具还应要求：
1） 采用联邦学习、安全多方计算等技术实现个人信息“可用不可见”；

2） 应部署自动化合规检查工具，识别资产化数据中的敏感字段（如身份证号、生物特征）。

7.3.1.4 数据资产化人员能力

在数据资产化阶段，对数据资产（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a） 应熟悉数据资产化过程相关安全管理的制度、流程，并基于制度、流程对数据资产进行安全管理；
b） 应能基于安全管理工具的信息对数据资产的安全性进行判断和分析；
c） 数据资产的安全审计人员应能基于制度对数据资产的安全管理合规性进行审计。

7.3.2 数据产品管理

7.3.2.1 数据产品组织管理

在数据产品开发阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全组织要求如下：

a） 组织应设立专职或兼职的岗位或人员负责以下工作：
1） 制定相关的数据产品开发安全管理制度，推动相关要求、流程的落地；
2） 对现有数据产品进行梳理和盘点；
3） 对数据产品规划过程中涉及的数据资源主体进行识别和安全性分析；
4） 对业务部门数据产品开发及管理过程的风险评估提供咨询和支持；
5） 对数据产品的合规性进行评估；
6） 对组织数据产品的梳理和盘点安全访问进行管理；
7） 对提取的数据产品特征信息并进行打标签处理；
8） 对数据产品的版本和存储进行管理；
9） 监管专业数据资产咨询公司、第三方会计事务所、律师事务所对数据的评估和分析；
10） 监督检查或审计数据产品管理的安全管理操作；
11） 负责明确组织在个人信息保护、重要数据保护、跨境数据传输等方面的安全合规需求，制定数据安全合规的规范要求和解决方案，推进其在组织整体范围内的执行。

b） 组织业务部门的业务团队安全要求如下：
1） 负责数据产品开发的安全管理；
2） 针对公共数据，还应要求：
- 设立公共数据安全管理组织，统筹产品设计、开发与安全合规性审查；
- 明确公共数据产品化责任组织，与第三方合作机构签订数据安全责任协议。

3） 针对企业数据，还应要求成立企业数据产品化安全决策组织，由法务、技术、业务部门联合审批产品方案；
4） 针对个人信息，还应要求：
- 设立个人信息保护组织，独立审查数据产品是否符合“最小必要”原则；
- 开发组织应负责定期审核数据产品中个人数据的分级、分类的合理性及风险评估。

7.3.2.2 数据产品制度建设

在数据产品开发过程中，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全开发制度要求如下：

a） 应建立数据产品规划安全评估和安全分析制度及流程；
b） 应制定数据产品的安全管理制度，管理制度应包含产品安全属性定义（如元数据的分类分级、数据主体类型以及敏感字段清单等）、过程安全管控要求（如开发阶段的隐私影响评估、发布审批的合规承诺书等）以及存储与交付安全（如产品存储位置的可信存储环境要求、产品的推出与审计机制）
c） 应针对第三方机构（专业数据资产咨询公司、会计师事务所、律师事务所）评估分析组织数据的授权、监督和管理制定相应的管理制度；
d） 应依据相关法律法规和标准，制定组织统一的数据跨境安全制度与管控措施；
e） 应从以下几方面管理数据产品的合规性

1） 应制定对数据产品的安全审计管理制度，包含数据产品的合规性安全审计以及数据产品管理安全性操作审计，并制定相关的审计频次和标准；
2） 明确组织所有的外部合规要求并形成清单，通过定期跟进监管机构合规要求的动态对该清单进行更新，同时将其拆分发送给相关方进行宣贯；
3） 应建立针对组织内部因业务架构、组织职能变更引发的重要数据流向变化的变更管控机制，以控制重要数据流向变化时可能引发的合规风险；
4） 应基于组织内部各类业务所涉及的在个人信息保护、重要数据保护、跨境数据传输等方面的合规风险，在组织整体的数据安全制度中明确针对个人信息保护、重要数据保护、跨境数据传输等方面的指导细则。

f） 针对公共数据，还应要求：
1） 建立公共数据产品化准入制度，禁止将未经脱敏的高敏感数据（如人口普查数据）直接用于商业化产品；
2） 制度中应明确公共数据产品化责任组织的职责，以及与第三方合作机构签订数据安全责任。

g） 针对企业数据，还应要求：
1） 建立企业数据产品化风险评估制度，对数据融合产生的衍生风险（如用户画像歧视）进行预判；
2） 制定数据产品生命周期管理制度，明确下架、召回机制（如发现产品存在隐私泄漏风险时）。

h） 针对个人信息，还应要求：
1） 遵循“单独告知—明示同意”制度，在用户使用数据产品前明确告知数据融合用途；
2） 依据个人信息保护相关法律法规与标准要求，制定组织统一的个人信息保护制度，构建符合相关要求的个人信息保护能力；
3） 在数据应用及关联业务组件下线和设备退网时，应妥善处理保存的个人信息（包括转存或销毁），避免因人员岗位调整、机构业务重组与兼并等原因违反个人信息保护要求；
4） 建立数据产品匿名化有效性验证制度，确保无法通过技术手段重新识别个人身份。

7.3.2.3 数据产品管理工具

在数据开发阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a） 应建立数据产品安全合规资料库，相关人员可以通过该资料库查询合规要求；
b） 应记录和保存第三方机构评估分析的结论性材料；
c） 应根据制度记录数据资源目录和数据资源被第三方机构使用的过程路径，形成数据资源访问闭环管理；
d） 应通过技术工具执行数据产品的管理，实现对数据产品的自动属性标识；
e） 应建立便于索引和查询的数据产品清单，并及时更新数据产品相关信息；
f） 应通过技术工具对数据产品进行可信安全的存储和查询；
g） 数据产品的访问和查询应留下访问痕迹，以便未来数据产品的安全审计；
h） 应量化组织整体的合规情况，并将合规结果通过图形化方式上报给管理层，以保证管理层有效了解组织整体合规情况；
i） 应建立组织统一的数据产品管理系统，通过技术工具实现对数据产品的统一管理，明确数据资产标识和数据资产相关管理方的属性标识；
j） 应通过数据资产产品管理系统量化组织内部数据产品的整体情况，包括但不限于数据产品的数据量、各等级数据产品的分布情况等，从而便于数据产品管理人员统计整体数据资产现状；
k） 应使用能对个人信息保护、重要数据保护、数据跨境传输的风险进行监控的技术工具，定期审核相关操作记录；
l） 应利用机器学习技术，对数据产品的状态（存储状态、备份状态、节点状态等）与访问记录进行分析，形成数据产品的安全性预警；
m） 应建立针对多源数据集汇聚和关联后个人信息利用的安全风险分析和保护控制措施；
n） 针对公共数据的开发安全管理工具还应要求采用动态脱敏技术，确保公共数据产品在测试、发布等环节中敏感信息不可还原；
o） 针对企业数据的开发安全管理工具还应要求采用数据加密传输技术（如 TLS 1.3），保障企业

数据产品在分发过程中的机密性；

p) 针对个人信息的开发安全管理工具还应要求：
   1) 采用同态加密技术实现数据产品计算过程中个人信息全程加密；
   2) 部署数据产品权限控制系统，支持基于角色的细粒度访问控制（如按字段级授权）。

7.3.2.4 数据产品人员能力

在数据开发阶段，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a) 负责该项过程的人员应具备对核心数据保护、重要数据保护、个人信息保护、跨境数据传输等方面的安全合规要求的解读和分析能力；
b) 熟悉组织产品化过程中的安全管理制度和流程以及相关的安全操作；
c) 开发人员应具备加密、解密、脱敏等相应知识及技能；
d) 针对公共数据，还应要求公共数据产品开发人员通过国家安全背景审查，并签署数据保密承诺书；
e) 针对个人信息的开发安全管理工具，还可要求个人信息产品运营人员通过隐私保护工程师（CISP—PIP）认证。

7.4 数据场景应用管理过程

7.4.1 数据服务管理

7.4.1.1 数据服务组织管理

在数据服务管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发安全组织要求：组织应设立专职或兼职的岗位或人员负责以下工作：

a) 对数据产品对外提供服务的数据进行分类分级；
b) 制定数据产品对外提供数据服务的制度和管理办法；
c) 负责统一的数据共享交换安全管理相关原则和技术能力的提供，并推动相关要求在相关业务中落地执行。

7.4.1.2 数据服务制度建设

在数据服务管理活动中，对数据（包含公共数据、个人信息以及企业数据）的开发制度安全要求如下：

a) 应基于数据分级、分类一般性要求，明确数据共享的原则和安全规范，明确数据共享目录、内容范围和数据共享的管控措施，数据共享涉及机构或部门相关用户职责和权限；
b) 应明确数据主体提供者与共享数据使用者的数据安全责任和安全防护能力；
c) 应明确数据共享审计规程和审计日志管理要求，明确审计记录要求，为数据共享安全事件的处置、应急响应和事后调查提供帮助；
d) 使用外部软件开发包/组件/源码前应进行安全评估，获取的数据应符合组织的数据安全要求；
e) 应在组织统一的数据共享原则基础上，明确主要数据共享场景的安全细则和审批流程，如对境外机构的数据共享安全细则、对政府机构的数据共享安全细则等；
f) 应定期评估数据共享机制、相关组件和共享通道的安全性；
g) 应在共享数据时，对数据接收方的数据安全防护能力进行评估；
h) 针对公共数据，还应要求建立公共数据服务场景准入制度，禁止提供未脱敏的原始敏感数据（如行政区划人口密度）；
i) 针对企业数据，还应要求制定企业数据服务黑名单，禁止通过 API 接口输出核心商业逻辑数据（如定价模型）；
j) 针对个人信息，还应要求：
   1) 遵循“最小化”原则，数据服务接口仅返回业务必需字段（如年龄区间代替具体出生日期）；
   2) 应针对含有个人数据的数据资源或产品提供的数据服务，制定相关制度审核个人数据分级、分类的合理性，并进行风险评估。

7.4.1.3 数据服务管理工具

在数据服务管理过程中，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工

具要求如下：

a) 应采取措施（如数据脱敏、数据加密、安全通道、共享交换区域等）确保不同等级数据在委托处理、共享、转让等对外提供场景的安全合规；
b) 应对共享数据及数据共享过程进行监控审计，共享的数据应属于共享业务需求且没有超出数据共享使用授权范围；
c) 应明确共享数据格式规范，如提供机器可读的格式规范；
d) 应建立组织统一的数据共享交换系统，提示数据共享交换的安全风险并进行在线审核；
e) 应配置数据共享机制或服务组件，明确数据共享最低安全防护要求；
f) 可建立数据产品服务的配置管理系统，实现基于数据产品元数据目录结构进行数据服务配置管理提供对外服务；
g) 针对公共数据的开发安全管理工具还应要求：
   1) 部署数据服务鉴权工具，防止未授权调用公共数据应用程序编程接口（Application Programming Interface, API）；
   2) 部署数据服务接口流量监控工具，实时检测异常调用行为（如高频访问、跨区域调用）。
h) 针对企业数据，还应要求部署数据产品使用监控工具，实时检测异常访问行为（如超量调用、跨区域访问）；
i) 针对个人信息，还应在数据服务接口中嵌入实时脱敏引擎，根据调用方权限动态返回脱敏后数据。

7.4.1.4 数据服务人员能力

在数据服务过程中，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a) 负责该项工作的人员应能充分理解组织的数据共享规程，并根据数据共享的业务执行相应的风险评估，从而提出实际的解决方案；
b) 可利用数据产品服务管理系统进行数据服务的配置管理；
c) 针对公共数据，还应要求公共数据流通操作人员通过国家安全部门备案，并定期接受数据跨境流通合规培训；
d) 针对企业数据，还应要求企业数据服务开发管理人员签订竞业禁止协议，离职后两年内不得从事同类数据业务；
e) 针对个人信息，还应要求个人信息处理人通过注册个人信息保护专员（Certified Information Security Professional-Personal Information Protection, CISP—PIP）认证。

7.4.2 数据可视化应用管理

7.4.2.1 数据可视化应用组织管理

在数据场景应用管理阶段，对数据（包含公共数据、个人信息以及企业数据）的开发安全组织要求如下：

a) 组织应设立专职或兼职的岗位或人员负责以下工作：
   1) 制定基于数据产品的场景化应用开发安全管理相关制度，推动相关要求、流程的落地；
   2) 对业务部门数据产品场景化应用开发的风险评估提供咨询和支持；
   3) 监督检查或审计数据产品场景化应用的安全管理操作。
b) 业务部门的安全团队应负责数据产品场景应用开发的安全管理。

7.4.2.2 数据可视化应用制度建设

在数据可视化应用活动中，对数据（包含公共数据、个人信息以及企业数据）的开发制度安全要求如下：

a) 应基于数据分级、分类一般性要求，明确数据可视化展示的原则、安全规范、内容范围和数据脱敏的管控措施，依据涉及机构或部门相关用户职责和权限，制定数据可视化应用制度；
b) 应明确数据提供者与数据可视化应用使用者的数据安全责任和安全防护能力；
c) 应明确数据可视化应用共享的数据产品审计规程和审计日志管理要求，明确审计记录要求，为数据可视化应用共享的安全事件处置、应急响应和事后调查提供帮助；

d) 使用外部的可视化软件开发包/组件/源码前应进行安全评估，获取的数据应符合组织的数据安全要求；
e) 应建立数据可视化分析过程的安全规范，覆盖构建数据仓库、建模、分析、挖掘、展现等方面的安全要求，明确个人信息保护、数据获取方式、访问接口、授权机制、分析逻辑安全、分析结果安全等内容；
f) 应建立数据可视化使用的评估制度，所有个人信息和重要数据的使用应先进行安全影响评估，满足国家合规要求后方可使用；数据的使用应避免精确定位到特定个人，避免评价信用、资产和健康等敏感数据，不得超出收集数据时所声明的目的和范围；
g) 应明确数据可视化分析安全审核流程，对数据分析的数据源、数据分析需求、分析逻辑进行审核，以确保数据分析目的、分析操作等的正当性；
h) 应采取必要的监控审计措施，确保实际进行的分析操作与分析结果使用与其声明的一致，整体保证数据分析的预期不会超过相关分析团队制定的数据权限范围；
i) 应定期评估数据可视化应用数据展示、相关组件和共享通道的安全性；
j) 应在共享数据时，对可视化应用数据接收方的数据安全防护能力进行评估；
k) 制度中有关可视化平台对公共数据、企业数据以及个人信息的展示，应参考7.4.1.2的要求处理。
l) 针对公共数据，还应要求建立公共数据服务场景准入制度，禁止可视化平台展示未脱敏的原始敏感数据（如行政区划人口密度）；
m) 针对企业数据，还可以要求制定企业数据服务黑名单，禁止通过可视化平台展示核心商业逻辑数据（如定价模型）；
n) 针对个人信息，还应对含有个人数据的数据可视化展示制定相关的制度审核个人数据的分级、分类的合理性，并进行风险评估；
o) 遵循“最小化”原则，可视化分析业务仅展示必需字段，对原始个人信息进行聚合分析后方可提供（如年龄区间代替具体出生日期）。

7.4.2.3 数据可视化应用管理工具

在数据可视化应用活动中，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全管理工具要求如下：

a) 应采取措施（如数据脱敏、数据加密等）确保不同等级数据在可视化应用场景下的安全合规；
b) 基于数据产品的数据服务，通过可视化应用配置实现可视化应用的权限管理；
c) 应结合技术手段（如基于机器学习的重要数据自动识别、数据安全分析算法设计等）降低数据分析过程中的安全风险；
d) 应采取必要的技术手段（如对分析结果数据进行扫描），并采取必要的控制措施和管理措施，避免输出的数据分析结果包含可恢复的个人信息、重要数据等数据和结构标识（如用户鉴别信息的重要标识和数据结构），防止数据分析结果危害个人隐私、公司商业价值、社会公共利益和国家安全；
e) 应依据数据合规要求建立相应强度或粒度的访问控制机制，限定用户可访问数据范围；
f) 应完整记录数据可视化分析使用过程的操作日志，以备对潜在违约使用者责任的识别和追责；
g) 应建立数据分析过程的安全风险监控系统，对数据分析可能涉及的安全风险进行批量的分析和跟进；
h) 可研究并利用新技术提升对用户的身份及访问管理能力，并通过风险监控与审计实现对数据使用的安全风险进行自动化分析和处理；
i) 针对公共数据，还可以要求在数据可视化平台中嵌入动态脱敏模块，确保敏感字段（如地理坐标）仅对授权角色可见；
j) 针对个人信息，还可以要求在数据服务接口中嵌入实时脱敏引擎，根据调用方权限动态返回脱敏后数据；
k) 针对个人信息，应采用多种技术手段以降低数据分析过程中的隐私泄露风险，如差分隐私保护、K匿名等；
l) 部署在线流通数据异常检测系统，识别并拦截批量下载、跨平台聚合等高风险行为。

7.4.2.4 数据可视化应用人员能力

在数据可视化应用过程中，对数据（包含公共数据、个人信息以及企业数据）的开发利用安全人员能力要求如下：

a) 负责该项工作的人员应能充分理解组织的数据共享规程以及数据可视化应用安全管理规程，并根据数据可视化的业务执行相应的风险评估，提出实际的解决方案；
b) 可利用数据产品服务管理系统进行数据可视化应用服务的配置管理；
c) 针对公共数据，还应要求公共数据流通操作人员通过国家安全部门备案，并定期接受数据跨境流通合规培训；
d) 针对个人信息，还应要求：
   1) 参与含有个人数据可视化应用的人员应了解个人信息的分级、分类，并熟悉含有个人数据的产品政策，以合法、合规的形式利用数据；
   2) 个人信息处理人应通过 CISP—PIP（注册个人信息保护专员）认证。

7.5 数据流通管理过程

7.5.1 数据服务交易管理

7.5.1.1 数据服务交易组织管理

在数据流通阶段以数据服务形式提供数据（包含公共数据、个人信息以及企业数据），其开发安全组织要求如下：

a) 产品供应方组织应设立专职或兼职的岗位或人员负责以下工作：
   1) 制定数据服务交易流通安全管理相关制度，推动相关要求、流程的落地；
   2) 对数据服务交易的安全风险进行评估并提供支持；
   3) 监督检查或审计数据服务交易的安全管理操作。
b) 政府部门应成立相应监管部门，负责以下公共数据监管工作：
   1) 基于国家相应法律法规，制定数据安全交易的相关政策和法规；
   2) 制定第三方可信存储服务、可信数据服务以及隐私计算服务的相关安全政策和法规；
   3) 制定数据跨境安全使用的数据安全使用政策；
   4) 监督管理数据的合法使用、数据流向以及数据跨境的安全使用。
c) 政府部门应组织成立具有国家公信力的单位注册并成为数据交易场所，负责以下工作：
   1) 建立数据交易平台，便于数据产品的上架、撮合、交易等数据流通活动；
   2) 对数据产品的分级、分类进行鉴定，确保符合国家、政府的安全分级、分类标准；
   3) 应引入数据商辅助数据交易场所数据流通；
   4) 可制定授信第三方可信存储服务、可信数据服务以及可信隐私计算相关服务的制度和办法；
   5) 可授信第三方可信存储服务、可信数据服务以及隐私计算相关服务；
   6) 可引入第三方隐私计算模型，包含但不限于人工智能模型、并行计算模型。
d) 数据产品供方、需方、数据商、第三方专业服务机构、数据交易场所等交易参与方，其对公共数据的开发安全组织基本要求应参考并满足 GB/T 37932—2024 中 6.1 的要求；
e) 数据产品供方还应参考并满足 GB/T 37932—2024 中 6.2 的要求；
f) 数据产品需方还应参考并满足 GB/T 37932—2024 中 6.3 的要求；
g) 数据商和第三方服务机构还应参考并满足 GB/T 37932—2024 中 6.4 的要求。

7.5.1.2 数据服务交易制度建设

在数据流通阶段以数据服务形式提供数据（包含公共数据、个人信息以及企业数据），其公共数据的开发制度要求如下：

a) 数据流通监管部门应制定以下相关数据交易安全政策和法规：
   1) 数据分级、分类的数据要素权益保护相关政策和法规；
   2) 公共数据的确权和授权相关法律法规；
   3) 数据市场化交易相关安全法律法规。
b) 数据交易场所应制定如下相关制度和办法：

1) 数据在线交易安全管理制度，明确交易主体、交易标的、交易平台、交易过程、交易安全、纠纷处理等交易规则、管理规范和服务指南；
2) 建立交易所内部数据安全制度，对交易所提供服务过程中收集和产生的数据进行安全管理，并规范数据交易相关人员的安全操作规则；
3) 应建立交易所信息报送和披露机制，及时披露数据交易行情、重大事项等信息，及时向市场主体提示数据交易风险，定期将数据交易情况报送相关监管部门；
4) 应建立完善数据交易主体信用评价制度，公示信用评价规则，为消费者提供对交易所上市售的交易标的进行评价的途径，且交易所不应删除消费者评价；
5) 应建立交易所数据交易管理制度、内部数据安全制度的制定、评审、发布流程，及时对制度内容进行更新完善，定期对制度落实情况进行监督；
6) 应建立数据交易合规巡检机制，定期对交易主体、交易标的的安全性、合规性进行检查；
7) 应定期开展数据安全风险评估和个人信息保护合规审计，并向有关部门报送风险评估报告和合规审计报告；
8) 应制定第三方可信存储服务、数据服务、隐私计算服务的相关安全管理制度和办法，支持数据的在线交易服务。

7.5.1.3 数据服务交易管理工具

在数据流通阶段以数据服务形式提供数据（包含公共数据、个人信息以及企业数据），其公共数据的开发利用安全管理工具要求如下：

a) 数据交易场所应建立数据交易平台，平台安全性基本要求如下：
   1) 应对交易过程进行安全管控，确保数据来源合法可确认、使用范围可界定、交易过程可追溯、安全风险可防范；
   2) 符合 GB/T 22239—2019 中第 3 级相关要求；
   3) 从事境内数据交易服务的数据交易平台，应部署在我国境内；
   4) 采用的密码技术应符合国家密码管理相关要求；
   5) 加强安全风险监测，发现安全缺陷、漏洞等风险时，立即采取补救措施。
b) 数据交易平台安全控制要求如下：
   1) 应对数据交易主体身份进行鉴别认证，并对用户进行权限管理和访问控制；
   2) 应允许对数据交易的参与方、对象、关键过程设置人工干预功能，人工干预内容至少包括交易参与方审核、交易数据和需求审核、交易暂停、交易撤销、交易恢复；
   3) 应提供交易合约的创建、上传、编辑、确认等功能，交易合约内容包括但不限于数据供方、数据需方、处理数据的算法逻辑或相关数据服务，数据的使用频次、使用期限、使用场景等；
   4) 可提供电子化交易合约模板，各交易主体对合约条款内容进行电子签名和确认；
   5) 应采用区块链技术对交易过程主要环节进行登记存证，记录交易参与方、交易标的、交易行为等信息，并确保存证信息不可篡改、不可伪造和可追溯性；
   6) 应授予数据交易各参与方所需的最小必要权限，实现各参与方的权限分离；
   7) 应对评估结果进行审核和记录，确保交易标的的安全性、合规性和数据质量。
c) 数据交易平台的安全审计要求如下：
   1) 应记录、保存平台发布的交易标的信息和交易信息，确保信息的完整性、保密性和可用性，交易标的信息和交易信息保存时间自交易完成之日起不少于三年；
   2) 交易信息应记录每笔数据交易信息，至少包括交易唯一标识、交易时间、供方、需方、交易标的、交易量、交易金额、交付方式、交易结果等；
   3) 应在数据交易平台运营过程中，记录交易主体、运营人员的操作处理、权限管理、交易过程等日志，日志留存时间不少于六个月；
   4) 应定期开展数据交易安全审计，仅允许授权审计人员访问数据交易日志，支持对数据交易日志进行查询和分析；
   5) 允许数据交易参与方查询与自己数据交易相关的日志信息，并允许导出；
   6) 支持监管方访问交易日志、数据存证、电子服务合约等审计资料，开展数据交易服务的安全监管工作；

7） 采取相应技术手段，对日志记录和安全审计结果进行保护，防止未授权篡改、破坏或泄露。

d） 数据交易平台应具备或集成第三方隐私计算能力、第三方可信存储服务以及可信数据服务，可针对数据的在线交易；

e） 数据交易平台的数据安全保护要求如下：

1） 应参考一般性安全要求中的数据传输安全要求，提供安全的数据传输通道，保证数据在传输过程中的保密性和完整性；

2） 应提供数据交付能力和安全稳定的数据交付环境，其中：应支持原始数据不出域、数据可用不可见的交付方式；应参考数据一般性安全要求，提供隔离安全环境，并采取数据加密、访问控制、数据防泄露、水印溯源、安全审计等措施，防止交易过程中的数据泄露、篡改、破坏或非法获取、非法交易、非法利用等；

3） 应为数据供方、需方提供安全的上传或下载接口，包括基于密码技术的身份认证、访问控制、传输链路加密、传输数据保密性和完整性校验等保护措施；

4） 应对数据交易平台接口的不安全输入参数进行限制和过滤，为接口提供异常处理能力；

5） 应为数据交易标的生成不可篡改的电子凭证，实现交易标的和交易操作的可追溯性及交易的不可否认性；

6） 应提供敏感数据识别和数据分类分级管理能力，根据交易标的的分类分级结果，对敏感数据进行识别和标注，并采用相应安全能力的数据流通安全保障技术进行交付；

7） 采取隔离存储、加密存储等措施，保障交易数据在存储过程中的保密性和完整性；

8） 提供数据交易平台的热冗余，支持本地数据备份恢复、异地实时备份等功能，保证系统和数据的高可用性；

9） 数据加工所涉算法的提供者应落实主体责任，加强算法安全管理，确保算法能维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益；

10） 具备恶意代码防护能力，能对交易数据含有的恶意代码进行检测。

f） 数据交易平台应根据数据的使用情况，利用机器学习统计分析数据的安全使用情况，并提供相关的安全警示；

g） 对在线 API 接口实施开放授权身份认证（Open Authorization, OAuth）、采用服务质量（Quality of Service）对流量限速以及 IP 白名单控制。

7.5.1.4 数据服务交易人员能力

在数据流通阶段以数据服务形式提供数据（包含公共数据、个人信息以及企业数据），对开发利用公共数据的人员能力要求如下：

a） 监管部门、交易场所开发人员、数据商、第三方服务机构开发人员、需方的开发人员、供方的开发人员均应具备如下能力：

1） 熟悉数据要素流通相关安全政策及相关法律法规；

2） 熟悉数据参与交易平台的相关安全管理制度和办法。

b） 监管部门还应熟悉数据要素流通的审计管理；

c） 交易场所开发人员安全还应：

1） 熟悉数据交易场所的相关安全制度和办法；

2） 熟悉数据交易平台的相关安全管理功能；

3） 应能根据数据交易后的数据交易情况对数据使用进行跟踪和溯源，并有针对性地对数据进行审计。

d） 需方开发人员的数据再加工后的数据资源化、产品化和场景应用能力应签署相关的安全管理要求；

e） 供方的开发人员还应能对数据的使用情况进行分析和追溯。

7.5.2 数据离线交易管理

7.5.2.1 数据离线交易组织管理

参考本文件7.5.1.1。

7.5.2.2 数据离线交易制度建设

在数据流通阶段以离线数据形式提供公共数据，其公共数据的开发制度要求如下：

a) 应参考本文件 7.5.1.2；
b) 应针对离线数据交易过程制定相关安全管理制度。

7.5.2.3 数据离线交易管理工具

在数据流通阶段以离线数据形式提供公共数据，其公共数据的开发管理工具要求如下：

a) 开发管理工具的安全要求参考 7.5.1.3，选择其中合理的安全要求；
b) 应能对静态的数据标的抽取唯一的特征码，并记录在可信的分布式账本中；
c) 可对交易数据标的添加电子水印，电子水印可用于溯源和数据使用追踪。

7.5.2.4 数据离线交易人员能力

在数据流通阶段以离线数据形式提供公共数据，其公共数据的开发人员能力参考7.5.1.4。

附 录 A
（资料性）
数据安全等级分类参考

A.1 数据安全级别确定规则

表 A.1 数据级别确定规则表

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

A.2 影响程度参考

表 A.2 影响程度参考示例表

影响对象	影响程度	参考说明
公共利益	特别严重危害	1) 关系重大公共利益，导致一个或多个省级行政区大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员（如1000万人以上）无法使用公共设施、获取公开数据资源、接受公共服务 2) 导致特别重大网络安全和数据安全事件，或者导致特别重大事故级别的安全生产事故，对公共利益造成特别严重影响，社会负面影响大 3) 导致特别重大突发公共卫生事件（I级），造成社会公众健康特别严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件
	严重危害	1) 直接危害公共健康和安全，如严重影响疫情防控、传染病的预防监控和治疗等 2) 导致重大突发公共卫生事件（Ⅱ级），造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件 3) 导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员（如100万人以上）无法使用公共设施、获取公开数据资源、接受公共服务
	一般危害	对公共利益产生一般危害，影响小范围社会成员使用公共设施、获取公开数据资源、接受公共服务等
组织权益	特别严重危害	导致组织遭到监管部门严重处罚（如取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产
	严重危害	导致组织遭到监管部门处罚（如一段时间内暂停经营资格或业务等），或者影响部分业务无法正常开展的情况，造成较大经济或技术损失，破坏机构声誉
	一般危害	导致个别诉讼事件，或在某一时间造成部分业务中断，使组织的经济利益、声誉、技术等轻微受损
个人权益	特别严重危害	个人信息主体遭受重大的、不可消除的、可能无法克服的影响，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。如遭受无法承担的债务、失去工作能力导致长期的心理或生理疾病、导致死亡等
	严重危害	个人信息主体遭受较大影响，个人信息主体克服难度高，消除影响代价较大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等
	一般危害	个人信息主体遭受困扰，但尚可以克服。如付出额外成本、无法使用应提供的服务造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等

参 考 文 献

[1] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[2] ISO/IEC 27001 Information technology—Security techniques—Information security management systems

[3] ISO/IEC 27040 Information technology—Security techniques—Storage security

[4] 《中华人民共和国个人信息保护法》（2021年8月20日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[5] 《中华人民共和国数据安全法》（2021年6月10日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[6] 《中华人民共和国网络安全法》（2016年11月7日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[7] 《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》（2025年1月6日国家发展改革委、国家数据局、中央网信办、工业和信息化部、公安部、市场监管总局联合制定）

[8] 《关于构建数据基础制度更好发挥数据要素作用的意见》（2022年12月2日中共中央、国务院发布）

[9] 《关于加快公共数据资源开发利用的意见》（2024年9月21日中共中央办公厅、国务院办公厅发布）

四 川 省 网 络 空 间 安 全 协 会

团 体 标 准

数据开发利用安全要求

T/CSAS 0020—2025

*

中国轻工业出版社出版

地址：北京鲁谷东街 5 号

邮政编码：100040

发行电话：(010)85119832

网址：http://www.chlip.com.cn

Email：club@chlip.com.cn

*

书号：155019·7145

印数：1—200 册　　定价：80.00 元