ICS 03.080.99
CCS M 19

DB5206

铜 仁 市 地 方 标 准

DB5206/T 175-2024

公共数据全生命周期安全管理规范

Public data lifecycle security management specification

2024-06-28 发布　　2024-09-28 实施

铜仁市市场监督管理局　　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。

本文件由铜仁市大数据发展管理局提出并归口。

本文件起草单位：铜仁市大数据发展管理局、贵州梵云大数据集团有限公司、中国电信股份有限公司铜仁分公司、铜仁学院大数据学院。

本文件主要起草人：赵　将、李宗亮、余　柔、陈　丹、陈进军、李正隆、田　波、鲁泓颍、万嘉华、李蔹育、杨胜明、杨　芬、万　勇、李　涛、邓明易。

公共数据全生命周期安全管理规范

1 范围

本文件规定了公共数据安全管理规范的术语和定义、原则和要求、通用安全要求、数据采集安全、数据传输安全、数据存储安全、数据使用安全、数据销毁安全。

本文件适用于铜仁市公共管理和服务机构对公共数据全生命周期的安全管理，其他数据的安全管理也可参照执行。

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 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

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

3.1

公共数据 public data

公共管理和服务机构在依法履职或提供公共服务过程中生产的，以一定形式记录或保存的文件、资料、图表、数据等各类数据资源，包括公共管理和服务机构直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的数据资源。

3.2

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。

3.3

数据合作方 data coperator

与公共管理和服务机构进行业务合作、提供技术支撑和数据服务等，并可能接触到公共数据的外部单位。

3.4

公共管理和服务机构 public management and service organization

铜仁市各级行政机关以及履行公共管理和服务职能的企事业单位和社会组织。

3.5

生命周期 life cycle

数据从采集到销毁的整个过程，指数据的采集、存储、传输、使用、销毁五个阶段。

4 原则和要求

4.1 安全原则

4.1.1 合法正当原则：公共数据采集应合法，不应窃取或者以其他非法方式获取，数据处理活动过程不应危害国家安全、公共利益，不应损害个人、组织的合法权益；

4.1.2 权责明确原则：采取技术和其他必要的措施保障数据的安全，对数据处理活动中涉及的组织和个人的合法权益负责；

4.1.3 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从其规定；

4.1.4 最小必要原则：数据处理活动仅处理可满足特定公共服务为目的所需的最少数据类型和数量；

4.1.5 公开透明原则：以明确、易懂和合理的方式公开公共数据处理的范围、目的、规则等，并接受外部监督，法律、行政法规另有规定的除外；

4.1.6 全程可控原则：采取必要管控措施确保公共数据全生命周期的可控性，记录数据处理各环节，防止未授权访问及处理公共数据。

4.2 安全要求

承载公共数据的信息系统应按 GB/T 22239 规定执行，数据处理过程涉及的密码技术应按 GB/T 39786 描述的密码应用基本要求执行。

5 通用安全要求

5.1 机构管理要求

5.1.1 建立组织层面的数据安全领导小组，由单位主要领导担任组长，分管领导担任副组长，中层干部为成员，并明确责任和义务；

5.1.2 明确组织内部的数据安全管理和监督部门，负责对组织内部的数据进行安全管理和监督；

5.1.3　建立数据安全管理制度，根据数据安全相关要求定期对制度的合理性和适用性进行论证和审定，并修订完善；

5.1.4　针对数据变更、重大数据操作及外部系统接入等重大事项建立审批程序，经数据安全管理和监督部门审核后，报数据安全领导小组组长审批；

5.1.5　建立数据安全追责问责机制，建立数据安全投诉、举报受理、处置制度。

5.2　人员管理要求

5.2.1　应加强人员管理，签订保密协议和竞业协议，明确数据访问范围、操作权限、违约责任等；

5.2.2　在选用重要岗位人员前应对其进行背景调查，符合相关的法律、法规要求；

5.2.3　明确重要岗位人员的数据安全培训计划，并在重要岗位变动环节对相关人员开展培训。

6　数据采集安全

6.1　数据采集的基本要求

6.1.1　按照一数一源、一源多用的要求，实现公共数据的一次采集、共享使用，可通过共享方式获得公共数据的，应避免通过其他方式采集数据；

6.1.2　明确数据采集过程重要数据的知悉范围和需要采取的控制措施，采取技术手段保证数据采集过程中重要数据不被泄漏；

6.1.3　依据统一的数据采集流程建设数据采集相关的工具，保证相关系统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。

6.2　数据采集的质量要求

6.2.1　规范数据采集的渠道、格式和方式，从而保证数据采集的合规性、完整性、实时性和一致性；

6.2.2　利用技术工具实现对关键数据进行数据质量管理和监控，对异常数据及时告警或更正；

6.2.3　对关键溯源数据进行备份，并采取技术手段对溯源数据进行安全保护；

6.2.4　建立疑义、错误信息快速校核机制，公共数据使用部门对获取的共享数据资源有疑义或发现有明显错误的，应及时反馈公共数据提供部门予以校核，错误的，应予以更正。

7　数据传输安全

7.1　数据传输基本安全要求

7.1.1　明确数据传输相关安全管控措施，如传输通道加密、数据内容加密等；

7.1.2　对数据传输两端进行身份鉴别，确保数据传输双方可信任；

7.1.3　采用校验技术保证数据在传输过程中的完整性。

7.2　网络安全性管理

7.2.1　制定网络安全性管理指标，包括安全性的概率数值、故障时间、统计业务单元等，建立基于安全性管理指标网络服务配置方案；

7.2.2　对关键的网络传输链路、网络设备节点实行冗余建设；

7.2.3　对网络安全性及数据泄漏风险进行防范，如负载均衡、防入侵攻击、数据防泄漏检测等设备和技术。

8　数据存储安全

8.1　数据存储基本安全要求

8.1.1　提供数据备份与恢复功能，同时考虑数据存储的保密性、完整性和多副本一致性；

8.1.2　归档数据建立安全保护机制；

8.1.3　建立数据逻辑存储隔离授权机制，具备多租户存储的安全隔离能力；

8.2　存储介质要求

8.2.1　明确存储媒介访问和使用的安全管理规范，建立存储媒介使用的审批和记录流程；

8.2.2　明确购买或获取存储媒介的流程，要求通过可信渠道购买或获取存储媒介，并针对各类存储媒体建立格式化规程；

8.2.3　建立存储媒介资产标识，明确存储媒介存储的数据；

8.2.4　使用技术工具对存储媒介性能进行监控，包括存储媒介的使用历史、性能指标、错误或损坏等情况。

8.3　数据备份和恢复

8.3.1　明确数据备份与恢复的管理制度，以满足数据的可靠性、可用性；

8.3.2　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、保存时长等；

8.3.3　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；

8.3.4　建立对过期存储数据及其备份数据彻底删除或匿名化处理的方法和机制，能够验证数据已被完全删除、无法恢复，并告知数据控制者和数据使用者；

8.3.5　通过风险提示和技术手段避免非过期数据的误删除，确保在一定的时间窗口内的误删除数据可以手动恢复。

9　数据使用安全

9.1　数据使用原则

9.1.1　明确数据使用的场景、目的和范围，建立数据使用过程的安全机制；

9.1.2　根据不同数据使用场景采用安全处理措施，降低数据敏感度及暴露风险；

9.1.3　依据数据使用目的建立访问控制机制，限定用户可访问数据范围，具备完整的数据使用操作记录；

9.1.4　数据使用过程中，具备风险监测和处理能力，对违规操作行为进行有效的识别。

9.2　数据共享安全

9.2.1　签署相关协议，明确数据使用目的、供应方式、共享范围、安全保护要求等内容；

9.2.2　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；

9.2.3　对请求共享的终端、用户或服务组件进行身份鉴别，验证身份的真实性；

9.2.4　对数据共享过程进行监控，确保共享数据安全合规，未超出授权范围；

9.2.5　采用数据加密、安全通道等安全措施保护共享过程中的数据。

9.3　数据开放安全

9.3.1　明确数据开放的审核制度，严格审核数据开放合规要求；

9.3.2　明确数据公开内容、适用范围及规范，明确发布者与使用者权利和义务；

9.3.3　定期审查开放的数据中是否含有非公开信息，并采取相关措施满足数据开放的合规性；

9.3.4　采取必要措施建立数据开放安全事件的应急响应和处置流程；

9.3.5　建立数据开放平台，实现公开数据登记、用户注册等验证互认机制。

10　数据销毁安全

10.1　数据资源的销毁

10.1.1　建立数据销毁与删除规程，明确数据销毁与删除场景、方式及审批制度，记录数据销毁与删除操作过程；

10.1.2　如因业务终止或组织解散，无数据承接方的，应及时有效销毁其控制的数据，法律、法规另有规定的除外；

10.1.3　委托数据合作方完成数据处理后，应要求数据合作方及时销毁委托的相关数据，法律、法规另有规定的除外；

10.1.4　使用规范的工具或产品，采用可靠技术手段及时销毁符合销毁条件的数据，确保数据不可还原。

10.2　存储介质的销毁

10.2.1　明确存储介质销毁处理方案、管理制度，明确销毁对象和流程；

10.2.2　依据存储介质存储内容的重要性，明确磁介质、光介质和半导体介质等不同类别存储介质的销毁方法；

10.2.3　明确对存储介质销毁的监控机制，确保对销毁存储介质的登记、审批、交接等销毁过程进行监控。