雄安新区数据安全建设导则

目　录

一、概述

（一）前言

依据《河北雄安新区智能城市建设专项规划》关于数据安全的总体要求，为实现雄安新区数据“可管、可控、可信”的目标，构建面向不同行业、领域的数据安全基础支撑体系，打造雄安新区全生命周期保障城市数据安全，创造安全的网络空间环境，需从数据准备、数据使用和数据评价三个阶段为新区的数据安全提供技术和管理保护，明确数据全生命周期环节中数据安全技术及其应用模式、密码和区块链等技术的创新性应用，形成从采集、传输、存储、处理、共享与交换到销毁的全流程数据安全技术要求，明确智能城市数据安全工程实现方法，规范新区未来城市与智能城市发展数据安全的顶层规划、体系化设计、建设实施等过程的相关要求，全面助力雄安新区发展和完善一体化的数据安全管控、防护和服务保障能力，特制定本导则。

（二）适用范围

本导则规定了雄安新区全区范围内党政机关和其他社会组织数据安全建设与发展相关的总体框架、技术要求和通用要求。

本标准适用于新区数据提供方、数据平台运营方、数据使用方和数据监管方的数据安全建设，对雄安新区党政机关和其他相关社会组织信息系统的数据安全保护和建设与发展提出基本要求。

（三）规范性引用文件

下列文件对于本文件应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 22240－2008《信息安全技术 信息系统安全等级保护定级指南》

GB/T 25069－2010《信息安全技术 术语》

GB/T 37988－2019《信息安全技术 数据安全能力成熟度模型》

GB/T 35274－2017《信息安全技术 大数据服务安全能力要求》

（四）术语定义

数据安全：通过管理和技术措施，确保数据有效保护和合规使用的状态。

数据交换：为满足不同平台或应用间数据资源的传送和处理需要，依据一定的原则，采取相应的技术，实现不同平台和应用间数据资源的流动过程。

数据共享：让不同数据用户能够访问大数据服务而整合的各种数据资源，并通过大数据服务或数据共享与交换技术对这些数据资源进行相关的计算、分析和可视化等处理。

二、数据安全总体策略要求

（一）数据基本保护策略

1.数据的访问控制策略

应针对数据正确授权操作的问题，通过建立正确的授权保证机制，保证对数据操作的授权，并保证授权的正确性。

2.数据的分属性、分级保护策略

应依据数据安全属性进行分类分级，为不同类别级别数据添加数据标签，对不同级别数据承载环境的提出安全要求。

3.数据安全传输策略

数据的安全传输依托于安全通信网络，本导则建议安全通信网络安全要求应满足但不限于《信息安全技术网络安全等级保护基本要求》中对安全通信网络的安全基本要求，并提出应对特殊数据（如控制信号与指令、密钥和校验码等）的安全传输建立相应的保护措施。

4.数据基本安全属性保护策略

采用安全管理策略和技术防护策略相结合，以及密码和区块链等创新型技术在数据安全中的应用保障数据的保密性、完整性、可用性、权属性、可溯源。

（二）数据安全防护策略

应以主动防御和综合防范为核心，根据实际业务需求，采用管理和技术相结合，建立可持续优化改进的数据安全管理运营机制，保障数据安全。

（三）数据全生命周期安全策略

数据安全管理应覆盖到数据从产生到销毁的全过程，应结合业务现状、系统安全现状、相关管理规范，形成从数据采集、传

输、存储、处理、共享与交换到销毁的全生命周期安全管理与技术要求。

（四）数据共享与开放策略

数据共享与开放需遵循以共享为常态，不共享为例外的原则，数据共享与开放不代表数据公开，在数据共享与开放过程中应确保敏感数据、个人隐私数据不被公开。数据共享与开放的策略应遵循数据分级分类实施差异化管控、敏感数据不被公开等原则。

（五）组织协调策略

应建立跨部门、跨单位的数据安全组织协同机制，通过明确分工、协同配合、强化执行、确保数据安全管理要求和技术防护要求的有效落地。

（六）合规评测策略

应建立定期内部安全检查机制，确保安全要求和防护手段有效落实。关注行业在数据保护方面的法规政策，不与相关法规政策相冲突。

三、数据安全建设总体要求

（一）数据安全阶段建设管理

本导则以数据全生命周期为基础，将数据安全建设划分为数据准备、数据使用和数据评价三个阶段，数据准备阶段包括数据采集、数据传输、数据存储、数据处理、数据销毁；数据使用阶段包括数据采集、数据传输、数据存储、数据处理、数据共享与交换、数据销毁；数据评价阶段主要针对数据准备阶段、数据使用阶段暴露的安全问题，制定一系列策略、流程、制度等来监督、

检查、协调多个相关职能部门，从而不断优化策略、方法、流程、工具、人员技能等，保障数据可管、可控、可信。

表 1 数据全生命周期角色权属

	数据提供方	数据平台运营方	数据使用方	数据监管方	数据全生命周期阶段	数据安全要求
数据准备阶段	√			√	数据采集安全	数据分类分级、数据标签、数据识别、数据采集身份管理、数据元鉴别及记录、资源目录管理、数据质量管理等
	√	√		√	数据传输安全	数据传输加密、网络可用性管理等
	√	√		√	数据存储安全	数据存储架构、存储媒体安全、逻辑存储安全、访问控制、数据备份和恢复、加密、数据溯源等
	√	√		√	数据处理安全	数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全等
	√	√		√	数据销毁安全	数据销毁处置、存储媒体介质销毁处置等
数据使用阶段		√	√	√	数据共享与交换安全	用户管理、授权管理、数据导出、数据导入、数据交换、数据共享安全、数据接口安全、数据发布安全等
		√	√	√	数据采集安全	数据分类分级、数据标签、数据识别、数据采集身份管理、访问控制、数据元鉴别及记录、资源目录管理、数据质量管理等
		√	√	√	数据传输安全	数据传输加密、网络可用性管理等
		√	√	√	数据存储安全	数据存储架构、存储媒体安全、逻辑存储安全、访问控制、数据备份和恢复、加密、数据溯源等
			√	√	数据处理安全	数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全等
		√	√	√	数据销毁安全	数据销毁处置、存储媒体介质销毁处置等
数据评价阶段				√	数据全生命周期	

（二）数据基础承载环境安全定级

为保障雄安新区数据的基础承载环境为数据安全提供基础的安全能力，本导则建议各数据承载平台应按照 GB/T 22240－2008《信息安全技术 信息系统安全等级保护定级指南》进行定级，并满足相应安全等级的安全要求。

四、数据全生命周期安全技术要求

（一）数据采集安全

1.数据分类分级

（1）应建立数据资产分类分级方法和操作指南，以确保数据资产分类分级的规范性和有效性。

（2）应建立数据资产清单，明确数据服务相关数据资产管理范围、属性及敏感程度。

（3）应依据数据资产和数据主体安全分级要求建立相应的标记策略，对采集数据进行分类分级识别和标识。

（4）应对不同类别和级别的采集数据实施相应的管理策略和保障措施。

（5）宜建立数据资产分类分级的变更审批流程和机制，以具备对数据分类分级变更操作进行合规定性审核的能力。

（6）宜依据数据分类分级策略变更对相关历史数据进行归档，并记录数据分类分级变更过程，确保数据分类分级过程的可追溯性。

（7）数据提供方应严格评估数据的敏感程度和安全级别，

以决定数据是否发送到区块链，是否进行数据脱敏，并采用严格的访问权限控制措施。

2.数据标签

（1）数据标签信息应包括但不限于：数据安全属性及相应等级、数据的所属部门与数据产生的时间和来源、数据的业务应用种类等。

（2）应建立覆盖结构化数据和非结构化数据范围的全量数据标签管理机制。

（3）结构化数据应建立基于数据字段名称基础上的数据内容指纹、数据分类、数据分级和敏感数据标识标签。

（4）非结构化数据应建立基于用户文件主体和文件属性信息基础上的文件内容指纹、数据分类和数据分级标签。

（5）应建立基于数据操作和数据访问基础上的用户行为标签，对操作异常和用户异常进行标识。

（6）应建立数据标签管理机制，对内外网的数据安全流转进行安全管控和追溯管理。

（7）数据标签应具备不容易被破坏或者删除的属性，敏感数据的数据标签应进行隐蔽性处理。

（8）应使用区块链机制对数据标签进行保护，防止数据标签的篡改、破坏和删除。

3.数据采集身份管理

（1）应制定数据采集最小化和合法化等原则，明确采集数

据的目的和用途，确保数据收集和获取的合法性和正当性。

（2）应明确数据收集和获取源以及数据收集范围和频度，确保数据收集和获取仅限业务所需的数据。

（3）应制定数据收集和获取操作规程，规范数据收集和获取渠道、数据格式、流程和方式。

（4）应对数据收集和获取环境（如采集渠道）、设施和技术采取必要的安全管控措施，确保采集数据的完整性、一致性和真实性。

（5）应确定数据收集和获取过程中个人信息和重要数据知悉范围和安全管控措施，确保采集数据的合规定性、完整性和真实性。

（6）应采用基于区块链的用户身份鉴权和访问控制策略，以保证用户身份不被篡改。

4.数据源鉴别及记录

（1）应明确数据源管理规范或制度，对采集的数据源进行鉴别和记录，以防止数据仿冒和数据伪造。

（2）应采用区块链机制确保数据处理过程中的操作日志和系统日志不会被篡改，以保证数据溯源过程的有效性和可信性。

5.数据质量管理

（1）应制定数据清洗、转换和加载操作相关的安全管理规范，确保清洗和转换前后数据间映射关系。

（2）应采取必要的技术手段和管理措施，确保在数据清洗、

转换和加载过程中对数据进行保护。

（3）应记录并保存数据清洗、转换和加载过程中个人信息、重要数据等数据的处理过程。

（4）应建立数据采集过程中质量监控规则，明确数据质量监控范围及监控方式。

（5）应定期对数据质量进行分析、预判和盘点，明确数据质量问题定位和修复时间要求。

（6）应利用技术工具实现对关键数据进行数据质量管理和监控，实现异常数据及时告警或更正。

（二）数据传输安全

1.数据传输加密

（1）应区分安全域内和安全域间不同的数据服务相应的数据传输场景，建立相应的数据传输安全策略和规程。

（2）应采用满足数据传输安全策略相应的安全控制措施，如安全通道、可信通道和数据加密等。

（3）应建立数据传输接口安全管理规范，包括安全域内和安全域间敏感数据传输接口规范。

（4）应具备在构建传输通道前对两端主体身份进行鉴别和认证的能力。

（5）应具备传输数据的完整性进行检测的能力以及相应的恢复控制措施。

（6）建立机制对数据传输安全策略的变更进行审核和监控，

包含对通道安全配置、密码算法配置和密钥管理等保护措施的审核及监控。

（7）应建立数据传输通道链路冗余机制，保证数据传输可靠性和网络传输服务可用性。

（8）应采用区块链机制，以保证信任证书验证服务器、客户端、专用网络和互联网之间系统访问者身份的合法性。

（三）数据存储安全

1.数据存储架构

（1）应建立开放可伸缩数据存储架构，以满足数据量持续增长和数据分类分级存储等需求。

（2）应制定数据存储架构相关的管理规范和安全规则，包括但不限于访问控制规则、存储转移安全规则、存储完整性和多副本一致性管理规则等。

（3）应采用必要的技术和管控措施保证数据存储架构安全管理规则的实施，确保数据存储完整性和多副本一致性真实有效。

（4）应确保存储架构具备对个人信息和重要数据等加密存储能力。

（5）应确保存储架构具备数据存储跨机构或跨机房容错部署能力。

（6）应采用基于区块链机制，以保证数据存储过程中数据防篡改。

2.存储媒体安全

（1）应明确存储媒体访问和使用管理规范，建立存储媒体使用审批和记录流程。

（2）应使用技术手段对存储媒体进行监控，包括但不限于存储媒体使用历史、性能指标、错误或损坏以及访问和使用行为等进行监控预警和记录审计。

3.逻辑存储安全

（1）应建立数据逻辑存储管理安全规范和机制，以满足不同数据类型、不同数据容量和不同业务需求的逻辑存储安全管理要求。

（2）应建立数据分片和分布式存储安全规范和规则，满足分布式存储下分片数据完整性、一致性和保密性保护要求。

（3）应明确数据逻辑存储隔离授权与操作规范，确保具备多租户数据存储能力安全隔离能力。

（4)应建立分层的逻辑存储授权管理规则和授权操作规范，具备对数据逻辑存储结构的分层和分级保护能力。

4.离线存储安全

（1）离线存储介质的保管场所应采用防火、防水、防磁和防尘等安全措施，配备可覆盖全部场地的防盗报警和视频监控等设施设备并确保设备正常运行。

（2）应统一规划数据离线存储的结构，按数据分类分级的结果进行分类集中存储，并留存存储结构说明文件。

（3）应采取措施确保离线存储数据安全、完整、可用。

（4）应及时记录离线存储介质的检测情况，包括检测结果是否正常、异常情况的处理措施和处理结果等。

（5）数据迁移后应按照数据销毁的相关要求对原离线存储介质进行销毁。

5.访问控制

（1）应建立基于属性的访问控制机制，根据用户的需求，以主体、客体和环境的属性为依据，配置具体的数据访问控制策略，并根据相应的访问控制策略划分不同的安全域。

（2）应建立存储系统安全管理员的身份标识与鉴别策略、权限分配策略和相关操作规范。

（3）应利用存储访问控制模块实施用户身份标识和鉴别策略、数据访问控制策略、数据扩容及复制策略等，实现相关安全控制措施。

（4）应具备数据分布式存储访问安全审计能力，建立受保护的审计信息存储机制和管控措施。

（5）应建立面向应用的安全控制机制，包含访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制。

（6）应建立数据存储安全主动防御机制或控制措施，如基于用户行为或设备行为安全控制机制。

（7）应利用区块链权限控制机制，对系统安全管理员进行身份鉴别和数据访问权限分配，具备防范单一节点受外部控制引

起的数据安全风险的能力。

6.剩余信息保护

（1）应明确剩余信息保护的对象，明确剩余信息的承载载体、以及需要保护的信息类型（如用户鉴别信息、用户拥有过的文件或目录、过程文件等）。

（2）应确保信息承载载体从一个客体释放并重新分配给另一个客体时，其中任何数据都不可被重用、恢复。

（3）应对内存数据进行剩余信息保护，对内存空间进行重新写入操作或对内存空间进行清零擦除。

7.数据备份和恢复

（1）应建立数据存储冗余备份恢复策略和管理规范，以满足数据服务可用性和可靠性等数据安全保护目标。

（2）应建立数据备份和恢复管理操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志记录和数据保存时长等。

（3）应建立数据备份与恢复的统一技术工具，并按照管理策略定期开展数据备份和数据恢复性测试，确保实现备份数据的可靠性和可用性的数据安全保护目标。

（4）应采用区块链机制保护数据备份和恢复的操作日志，防止相关日志信息被篡改。

8.加密

（1）在智能城市中对涉及国家秘密信息的数据进行传输、

存储和处理时，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护，保障数据的机密性和完整性。

（2)在智能城市中对不涉及国家秘密的重要数据进行传输、存储和处理时，应当依照法律、行政法规和国家有关规定使用商用密码进行加密保护，保障数据的机密性和完整性。

（3）应按照数据的分类分级结果，对不同安全等级的数据分别进行存储加密保护。

（4）在大数据环境下，应建立相对应的数据加密处理策略和规范，平衡数据处理的机密性和可用性需求。

（5）应建立统一密钥管理体制，实现数据加密和数据解密密钥的安全分发和管理，并支持对云计算环境下的密钥进行统一管理。

9.数据溯源

（1）应制定数据溯源策略和溯源机制，以及溯源数据安全存储与使用的管理制度。

（2）应制定溯源表达方式和格式规范，以规范化组织、存储和管理溯源数据。

（3）应采用必要的技术手段和管控措施实现分布式数据处理环境下溯源数据采集和存储，确保溯源数据能重现数据处理过程，如追溯操作发起者及发起时间。

（4）应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。

（5）应采取技术手段和管控措施保证溯源数据的完整性和保密性。

（6）应建立基于溯源数据的数据业务与法律法规合规性审核机制，并依据审核结果增强或改进数据服务相关的访问控制与合规性保障机制和策略。

（7）应对结构化数据及非结构化数据进行敏感度识别，并建立数据追溯策略、追溯管理机制以及追溯数据安全存储与使用的管理制度。

（8）应对结构化数据及非结构化数据的敏感字段进行数据血缘分析，明确数据的来源及数据在流转中的处理过程。

（9）应对应用系统中敏感数据的源头进行溯源，对敏感数据的流动进行追踪，并能针对单个或多个的敏感数据流转形成完整的追溯链条，建立数据血缘关系图。

（10）应对多个应用系统之间流转的敏感数据能进行溯源和追踪管理，并能针对敏感数据流转形成完整的追溯链条，追溯链条包括但不限于对用户输入的字段、用户接口、应用接口、数据调用接口和数据库接口等。

（11）数据追溯过程应对关联的数据操作日志和用户访问行为信息进行关联，以便进行审计和取证。

（12）应建立数据追溯管理机制，实现静态、存储和传输中数据的血缘关系以及数据族系的可视化管理。

（13）应采取技术手段和管控措施保证追溯数据的完整性和

保密性。

（14）应采用区块链机制，以确保数据存储过程中的操作日志和系统日志不会被篡改。

（四）数据处理安全

在数据使用阶段，数据使用方、平台运营方和数据监管方应在各自职责范围内采取相应技术措施保障数据处理安全，具体包括:

1.数据脱敏

（1）应建立数据脱敏管理规范和制度，明确数据脱敏规则、脱敏方法和使用限制。

（2）应明确数据脱敏处理应用场景、数据脱敏处理流程和涉及部门及人员的职责分工。

（3）应配置数据服务组件或技术手段，支持如泛化、抑制和干扰等数据脱敏技术。

（4）应能够在屏蔽信息时保留其原始数据格式和特定属性，以满足基于脱敏数据的开发和测试要求。

（5）应对数据脱敏处理过程相应的操作进行记录，以满足数据脱敏处理安全审计要求。

（6）应明确列出需要脱敏的数据资产以及字段，给出不同分类分级数据的脱敏处理流程和脱敏方式。

（7）应配置或部署脱敏数据识别和脱敏效果验证服务组件或技术手段，确保数据脱敏的有效性和合规定性。

（8）应明确数据治理原则和规范。

（9）应配置基于策略的数据脱敏支持服务组件或管控措施。

（10）应建立基于区块链的溯源数据摘要机制，支持对溯源数据进行验证，确保溯源数据的一致性。

2.数据分析安全

（1）应建立数据分析相关数据源获取规范和使用机制，明确数据获取方式、访问接口、授权机制和数据使用等。

（2）应建立多源数据派生、聚合和关联分析等数据分析过程中的数据源源操作规范和实施指南。

（3）应建立数据分析结果输出的安全审查机制和授权控制机制，并采取必要的技术手段和管控措施保证共享数据分析结果不泄露个人信息和重要数据等敏感信息。

（4）应对数据分析结果共享的风险进行合规定性评估，避免分析结果输出中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。

（5）应对数据分析过程中个人信息和重要数据等敏感数据操作进行记录，以实现对分析结果质量和真实性进行追踪溯源。

3.数据正当使用

应确保数据使用和分析处理的目的和范围符合网络安全法等国家相关法律法规要求。

4.数据导入导出安全

（1）应综合数据量、增长速度、业务需求和性能等因素制

定数据导入导出管理策略和规程。

（2）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授权策略、不一致处理策略和流程控制策略。

（3）应依据数据导入导出策略与规程和授权策略等，建立数据导入导出安全评估机制和授权审批流程。

（4）应对数据导入导出终端、用户或服务组件等执行身份鉴别，验证期身份的真实性和合法性。

5.数据处理环境安全

（1）数据处理环境的系统设计、开发和运维阶段应制定相应的安全控制措施，确保对安全风险的管控。

（2）应明确数据处理环境的安全管理要求。

（3）应基于数据环境建立分布式处理安全要求，对外部服务组件与使用审核、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、敏感数据发现与脱敏、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。

（4）应明确适合数据处理环境的数据加解密处理要求和密钥管理要求。

（5）数据处理与数据权限管理机制应实现联动，用户在使用数据的系统前已获得了授权。

（6）基于数据处理的多租户特性，应对不同的租户保证其在系统中的数据、系统功能、会话、调度和运营环境等资源实现

隔离控制。

（7）应建立数据处理日志管理机制，记录用户在数数据处理上的加工操作，提供数据在系统上加工计算的关联关系。

（8)应针对用户在数据处理上对数据的操作开展定期审计，确定用户对数据的加工未超出前期申请数据时的目的。

（五）数据共享交换安全

1.用户管理

应根据业务需求、管理范围和组织架构等设立访问控制策略，建立完整的用户管理机制，能够统一设立、统一注销、统一鉴别、统一授权、集中鉴权和集中审计。

2.授权管理

（1）应提供针对用户访问权限、数据操作权限和应用访问数据权限等维度的授权管理机制。

（2）应支持基于数据分级分类的多级授权和操作监管。

（3）应对权限范围外的数据和应用尝试操作提出告警。

（4）应支持文件数据、表数据项和接口等不同粒度权限控制。

（5)共享资源发布/申请应获得授权，明确授权目的和范围，保留授权记录，并遵照授权执行。

（6）应根据安全策略，生成共享资源访问授权凭证和安全配置信息，并将这些信息安全分发到信息共享与交换中。

3.数据共享

（1）应对每次数据共享指定具有唯一性的共享与交换事务标识。

（2）应对数据共享两端进行用户身份鉴别或设备认证，确保数据共享与交换两端身份的真实性。

（3）应检查对使用方数据共享操作的授权，并遵照授权策略执行访问控制，拒绝不符合授权的访问，保留授权检验记录。

（4）在共享与交换敏感类数据时，应由数据提供方对发出数据和时间戳进行数字签名，数据使用方应校验数据提供方数字签名的合法性。

（5）应跟踪和记录数据共享全过程，确保溯源记录能满足溯源过程需要。

4.数据交换安全

（1）应明确数据交换内容范围和数据交换管控措施。

（2）应审核共享数据的数据内容，确保属于满足数据交换业务场景需求范围。

（3）应建立共享数据格式规范，如提供机器可读的格式规范，确保高效获取共享数据。

（4）应定期评估数据交换机制、服务组件和共享通道安全性。

（5）应配置专业数据交换机制或服务组件，明确数据交换最低安全防护基线要求。

（6）应通过公钥对机构用户的身份进行标识，应通过数据

指纹对数据进行标识。

（7）应通过区块链共识网络实现用户的安全接入、发布验证、数据确权、读取控制、数据评价和共享确责。

（8）应通过区块链浏览器对网络节点及共享数据的态势进行呈现，整个区块链数据均是通过哈希进行串联，确保数据的不可篡改，同时可以通过数据指纹对数据交换记录进行关联查询，通过签名确保查询结果的不可抵赖，通过交易编号确保数据的不可抵赖。

（9）应采用区块链机制，以确保数据交换过程中的操作日志和系统日志不被篡改。

5.数据开放安全

（1）应建立数据资源公开的审核制度和规范，严格审核数据发布业务，以确保符合国家相关法律法规要求。

（2）应明确数据资源公共内容、适用范围及规范，明确发布者与使用者权利和义务。

（3）应依法公开数据服务相关数据资源公告、资格审查、成交信息和履约信息等数据发布信息。

（4）应建立数据资源公开事件应急处理流程，包括保障处理流程快速有效的必要措施。

（5）应建立数据资源公开数据库，通过数据发布服务实现公开数据资源的登记和用户注册等共享数据及共享组件的验证互认机制。

（6）应指定专人负责数据发布信息的披露，并能对数据披露人员进行相应的安全培训。

（7）应定期审查公开发布的数据资源中是否包含非公开信息，并采取相关措施确保发布数据使用的合规性。

（8）应建立数据资源发布接口以及发布数据格式规范，如提供机器可读的可扩展标记语言格式，确保用户能高效获取开放数据资源。

（9）应通过公钥对机构用户的身份进行标识，通过数据指纹对数据进行标识。

（10）应通过区块链对发布数据做唯一性鉴别。

6.数据接口安全

（1）应制定数据服务接口安全控制策略，明确规定使用服务接口的安全限制和安全管制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳和安全协议等。

（2）应明确数据服务接口安全规范，包括但不限于接口名称、接口参数和接口安全控制要求等，具备对接口不安全输入参数进行限制或过滤能力，为接口提供异常处理能力。

（3）应具备服务接口访问的审计能力，并能为数据安全审计提供可配置的数据服务接口。

（六）数据销毁安全

1.数据销毁处置

（1）应建立数据销毁策略和管理规范，明确销毁对象和流

程，并依照数据分类分级建立相应的数据销毁机制，明确销毁方式和销毁要求，对数据销毁进行审计，设置销毁相关监督角色，监督销毁操作过程。

（2）应配置必要的数据销毁技术手段和管控措施，确保以不可逆方式销毁数据及过期副本内容。

（3）应按照国家相关法律法规和标准销毁个人信息和重要数据等敏感信息。

2.存储媒体介质销毁处置

应建立存储媒体介质销毁处理策略、管理制度和机制，明确销毁对象和销毁流程。

五、数据安全通用要求

（一）策略和规程

建立适用于雄安新区的数据安全策略和规程，包含数据安全的目标、范围、原则等；并根据不同管理制度，针对相应管理人员或操作人员执行日常管理操作建立相应操作规程，具体安全要求可参考 GB/T 35274－2017《信息安全技术大数据服务安全能力要求》中对策略和规程的相关安全要求。

（二）组织和人员管理

建立负责数据安全工作的职能部门及岗位，明确各岗位的安全职责，并对人力资源管理过程中各环节进行安全管理，防范组织和人员管理过程中存在的数据安全风险，具体安全要求可参考 GB/T 35274－2017《信息安全技术大数据服务安全能力要求》中

对组织和人员管理的相关安全要求。

（三）元数据管理

建立组织的元数据管理体系，实现对元数据的集中管理，具体安全要求可参考 GB/T 37988－2019《信息安全技术 数据安全能力成熟度模型》中对元数据管理的相关安全要求。

（四）数据供应链管理

建立数据供应链安全管理规范和安全方针，明确数据供应链安全目标、安全原则和范围，具体安全要求可参考 GB/T 35274－2017《信息安全技术大数据服务安全能力要求》中对数据供应链管理的相关安全要求。

（五）合规性管理

制定策略和规程确保数据安全的各项措施满足合规要求，具体安全要求可参考 GB/T 35274－2017《信息安全技术大数据服务安全能力要求》中对合规性管理的相关安全要求。

（六）监控与审计

实现对各数据支撑平台数据全生命周期的安全审计，并保证审计记录不可伪造和篡改，具体安全要求可参考 GB/T 37988－2019《信息安全技术 数据安全能力成熟度模型》中对监控与审计的相关安全要求。

（七）终端数据安全

制定对终端设备的数据保护技术要求及管理要求；具体安全要求可参考 GB/T 37988－2019《信息安全技术 数据安全能力成

熟度模型》中对终端数据安全的相关安全要求。

（八）安全事件应急

建立针对数据的安全事件应急响应体系；具体安全要求可参考GB/T 37988－2019《信息安全技术 数据安全能力成熟度模型》中对安全事件应急的相关安全要求。

（九）数据资产管理

建立对数据资产的有效管理手段，从资产类型和管理模式方面实现统一的管理要求；具体安全要求可参考GB/T 37988－2019《信息安全技术 数据安全能力成熟度模型》中对数据资产管理的相关安全要求。

（十）数据管理总体要求

应制定相应的数据管理制度，以保证保障个人信息和重要数据安全，明确数据管理的范围和不同数据管理者的职责，以防止数据的误用、丢失和破坏。

（十一）数据资源目录建设

具体要求可参考《雄安新区数据资源目录》相关管理规范要求。

（十二）数据开放共享管理

应由管理层对数据开放共享进行统一管理，负责数据开放共享规范的制定和实施应按照相关法律法规，制定统一的内外部数据共享互通的政策和规范等，包括安全、质量和数据口径等内容。

（十三）数据标准要求

1.应明确数据标准制定过程中的要求，以保证数据标准的规范性和可实施性;

2.应建立健全的数据标准的评审制度，以保证最终指定的数据标准的质量。

（十四）密码管理

在智能城市中对数据进行传输、存储和处理时，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护，保障数据的机密性和完整性。并建立统一的密钥管理体制，实现数据加密和数据解密密钥的安全分发和管理，并支持对云计算环境下的密钥进行统一管理。

（十五）个人信息保护

《中华人民共和国个人信息保护法》正在制定中，相关安全要求应遵循未来法律法规相关内容。