ICS 35.040

L80

DB15

内蒙古自治区地方标准

DB 15/T XXXXX—XXXX

|  |
| --- |
|  |

公共大数据安全管理指南

Public Big Data Security Management Guide

|  |
| --- |
| 征求意见稿 |
|  |

XXXX-XX-XX发布

XXXX-XX-XX实施

目  次

[前  言 III](#_Toc14267106)

[引  言 IV](#_Toc14267107)

[1 范围 1](#_Toc14267108)

[2 规范性引用文件 1](#_Toc14267109)

[3 术语和定义 1](#_Toc14267110)

[4 概述 2](#_Toc14267122)

[4.1 数据生命周期的各个阶段 2](#_Toc14267123)

[4.2 数据安全体系 3](#_Toc14267124)

[5 通用安全 4](#_Toc14267125)

[5.1 数据安全策略规划 4](#_Toc14267126)

[5.2 组织和人员管理 4](#_Toc14267127)

[5.3 个人信息保护 5](#_Toc14267128)

[5.4 数据资源目录 5](#_Toc14267129)

[5.5 数据供应链安全 6](#_Toc14267130)

[5.6 元数据管理 7](#_Toc14267131)

[5.7 终端数据安全 7](#_Toc14267132)

[5.8 监控与审计 7](#_Toc14267133)

[5.9 鉴别与访问控制 8](#_Toc14267134)

[5.10 需求分析 8](#_Toc14267135)

[5.11 安全事件应急 9](#_Toc14267136)

[5.12 敏感数据保护 9](#_Toc14267137)

[6 安全监管 9](#_Toc14267138)

[7 数据采集安全 10](#_Toc14267139)

[7.1 数据分类分级 10](#_Toc14267140)

[7.2 数据采集安全管理 10](#_Toc14267141)

[7.3 数据源鉴别及记录 11](#_Toc14267142)

[7.4 数据质量管理 11](#_Toc14267143)

[8 数据传输安全 12](#_Toc14267144)

[8.1 数据传输加密 12](#_Toc14267145)

[8.2 网络可用性管理 12](#_Toc14267146)

[9 数据存储安全 12](#_Toc14267147)

[9.1 存储媒介安全 12](#_Toc14267148)

[9.2 逻辑存储安全 13](#_Toc14267149)

[9.3 数据备份和恢复 13](#_Toc14267150)

[10 数据使用安全 14](#_Toc14267151)

[10.1数据脱敏 14](#_Toc14267152)

[10.2 数据分析安全 15](#_Toc14267153)

[10.3 数据正当使用 15](#_Toc14267154)

[10.4 数据处理环境安全 16](#_Toc14267155)

[10.5 数据导入导出安全 16](#_Toc14267156)

[11 数据交换安全 17](#_Toc14267157)

[11.1数据共享安全 17](#_Toc14267158)

[11.2 数据开放安全 17](#_Toc14267159)

[11.3 数据接口安全 18](#_Toc14267160)

[12 数据退役安全 18](#_Toc14267161)

[12.1 数据归档和转移 18](#_Toc14267162)

[12.2 数据退役处置 18](#_Toc14267163)

[12.3 存储媒介销毁处置 19](#_Toc14267164)

[参考文献 19](#_Toc14267165)

前  言

本标准依据GB/T1.1—2009给出的规则进行起草。

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。

本标准由内蒙古自治区大数据发展管理局提出并归口。

本标准起草单位：内蒙古自治区大数据发展管理局，中国电子技术标准化研究院。

本标准主要起草人：全鑫，孙卫，刘贤刚，胡影，张宇光，刘朝苹。

引  言

为了加强公共数据安全管理，维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，促进公共数据资源开发利用，推动实施大数据战略，根据《中华人民共和国网络安全法》等相关法律法规和国家政策规定，结合本自治区实际，制定本标准。

涉及国家秘密的公共数据安全管理，按照有关保密法律法规的规定执行。

公共大数据安全管理指南

1. 范围

本标准从数据生命周期、通用安全管理和安全监管三个方面，提出内蒙古自治区公共大数据安全管理指南。

本标准适用于规范公共管理和服务机构开展公共数据采集、存储、传输、使用、共享、开放、退役等数据活动，也可为内蒙古自治区有关部门对数据活动进行监督管理提供参考。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所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 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 35274　信息安全技术　大数据服务安全能力要求

1. 术语和定义

GB/T 25069中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行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和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等。

3.2  
 公共管理和服务机构 public management and service organization

内蒙古自治区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，涉及公共数据开发的产业机构。

3.3  
 大数据 big data

具有数量巨大、种类多样、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理技术进行有效组织、存储、计算、分析和管理的数据集。

3.4  
 重要数据 important data

是指不涉及国家秘密，但如果泄露、毁损、丢失或被窃取、篡改和非法使用可能危害国家安全、国计民生、公共利益的未公开数据。

3.5  
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识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：关于个人信息的范围和类型可参见GB/T 35273《信息安全技术 个人信息安全规范》附录A。

3.6  
 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信息的一种数据保护方法。

3.7  
 大数据平台　big data platform

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件集合，包括监视大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

3.8  
 数据活动 data activity

组织机构针对数据开展的一组特定任务的集合，数据活动主要包括采集、存储、传输、使用、共享、删除等。

3.9  
 数据供应链　data supply chain

为满足数据供应关系，通过资源和过程将需方、供方相互连接的网链结构，可用于供方将数据及其产品与服务提供给需方。

3.10  
 组织机构 organization

由作用不同的个体为实施共同的业务目标而建立的结构。组织可以是一个企业、事业单位、政府部门等。

注：本标准的组织机构，通常是指公共管理和服务机构。

3.11  
 合规　compliance

对数据安全所适用的法律法规的遵循。

1. 概述

4.1 数据生命周期的各个阶段

本标准定义了数据生命周期的六个阶段，并针对公共数据特点和场景进行了描述：

1. 数据采集：组织机构内部系统中新产生数据，以及从外部系统收集数据的阶段。在公共数据方面，通常是指公共管理和服务机构因履职需要，采用直接采集、委托第三方机构采集、协商等方式向公民、法人和其他组织获取有关数据，以及通过业务系统、监测、测量、录音、录像等方式产生有关数据。
2. 数据传输：数据从一个实体通过网络流动到另一个实体的阶段。在公共数据方面，通常是公共管理和服务机构将数据传输归集到云平台、数据资源共享交换平台、大数据中心等，下一级部门将公共数据传输汇聚到上一级部门等。
3. 数据存储：数据以任何数字格式进行物理存储或云存储的阶段。在公共数据方面，数据存储可能涉及采集数据存储、归集汇聚后的数据存储、数据共享交换后的数据存储等。
4. 数据使用：组织机构针对数据进行计算、分析、可视化等操作的阶段。在公共数据方面，通常是对公共数据进行整合，形成基础数据库和主题数据库，并进行大数据分析利用转化成公共大数据产品或服务。
5. 数据交换：组织机构与组织机构及个人进行数据共享、开放、交换的阶段。公共数据共享通常是公共管理和服务机构因履行职责需要使用其他公共管理和服务机构公共数据，并为其他公共管理和服务机构提供公共数据。公共数据开放通常是公共管理和服务机构通过数据开放平台向社会开放公共数据。公共数据交换通常是公共管理和服务机构间或公共管理和服务机构与个人进行数据交互。
6. 数据退役：不再进行处理的公共数据进入数据退役阶段，涉及对信息的归档、转移、丢弃、销毁以及对存储介质的销毁处理等。

特定的数据所经历的生命周期由实际的业务场景所决定，并非所有的数据都会完整地经历六个阶段。

4.2 数据安全体系

公共数据安全体系由30类安全技术和管理控制措施组成，分成数据生命周期安全、通用安全、安全监管三部分，如图1所示。其中数据生命周期安全包含数据采集、数据传输、数据存储、数据使用、数据交换、数据退役六个阶段的安全措施。安全通用安全是指对数据生命周期各阶段通用的安全技术和管理措施。安全监管则是从公共数据主管部门角度提出的安全监管类措施。其中，安全监管是数据生命周期安全建设中必须被满足的基线要求，通用安全是数据生命周期安全建设的中具有共性的安全建设内容，一般贯穿于数据全生命周期建设，三者共同构建了公共数据安全体系。



1. 数据安全体系
2. 通用安全

5.1 数据安全策略规划

建立组织机构整体的数据安全策略规划，数据安全策略规划的内容应覆盖数据全生命周期的安全风险。

公共服务和管理机构应：

1. 设立负责组织机构数据安全制度流程和战略规划的建设的岗位和人员。
2. 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。
3. 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，覆盖数据生命周期相关的业务、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。
4. 明确并实施大数据系统和数据应用安全实施细则。
5. 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。
6. 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。
7. 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。
8. 确保负责制定数据安全总体策略和战略规划的人员了解组织的业务发展目标，能够将数据安全工作的目标和业务发展的目标进行有机结合。
9. 确保负责制定数据安全制度和规程的人员具备信息安全管理体系建设的知识，并具备良好的规范撰写能力。
10. 确保负责推广数据安全策略规划的人员能够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。

5.2 组织和人员管理

通过建立组织机构内部负责数据安全工作的职能部门及岗位，以及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。

公共服务和管理机构应：

1. 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，并明确了组长的责任与权力。
2. 建立组织层面专职的数据安全职能部门和岗位，明确其工作职责，以及职能部门之间的协作关系和配合机制，并在职能岗位设计时考虑职责分离的原则。
3. 确保人力资源部门与负责数据安全的部门能够进行有效配合。
4. 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。
5. 指定大数据系统的安全规划、安全建设、安全运营和系统维护工作的责任部门。
6. 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。
7. 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。
8. 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。
9. 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。
10. 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。
11. 在录用重要岗位人员前对其进行背景调查，符合相关的法律、法规、合同要求，对数据安全员工候选者的背景调查中也包含了对候选者的安全专业能力的调查。
12. 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。
13. 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。
14. 在重要岗位人员调离或终止劳动合同前，与其签订保密协议或竞业协议。
15. 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。
16. 明确重要岗位人员的数据安全培训计划，并在重要岗位转岗、岗位升级等环节对相关人员开展培训。
17. 及时终止或变更离岗和转岗员工的数据操作权限，并及时将人员的变更通知到相关方。
18. 按最少够用原则为入职员工分配初始权限。
19. 以公开信息且可查询的形式，面向组织全员公布数据安全职能部门的组织架构。
20. 确保负责组织和人员管理的人员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。
21. 开展针对员工入职过程中的数据安全教育，通过培训、考试等手段提升其整体的数据安全意识水平。
22. 负责设置数据安全职能的人员，能够明确组织的数据安全工作目标。

5.3 个人信息保护

针对个人信息保护的合规要求，建立个人信息保护措施，防止个人信息保护的合规风险。

公共服务和管理机构应：

1. 梳理组织机构所有的个人信息保护合规要求并形成清单，能够定期通过跟进监管机构合规要求的动态对该清单进行更新。
2. 依据个人信息保护相关法律法规和GB/T 35273《信息安全技术 个人信息安全规范》的要求，制定组织机构统一的个人信息保护制度规范，建立符合国家法律法规和相关标准的个人信息保护能力。
3. 在传输和存储个人敏感信息时，采用加密等安全措施。
4. 在存储个人生物识别信息时，采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅存储摘要信息。
5. 对被授权访问个人信息的人员，建立最小授权的访问控制策略，使其只能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限。
6. 确保涉及通过界面展示个人信息（如显示屏幕、纸面）时，个人信息控制者对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。
7. 按照法律法规相关要求，采取措施保障用户对个人信息的查询、更正、删除等权益。
8. 确保通过注册账户提供服务时，向个人信息主体提供简便易操作的注销账户方法。

5.4 数据资源目录

通过建立针对公共数据资源目录的有效管理，从资源类型、管理模式方面实现统一规范。

公共管理和服务机构应：

1. 实行公共数据统一目录管理，明确公共数据的范围、数据提供单位、更新时限、格式、共享开放属性等要素。
2. 根据相关政策标准要求，编制、更新、维护和发布本部门公共数据资源目录，并纳入全区公共数据资源目录。如有关法律法规规章作出修订或职能职责发生变化，应及时更新本部门公共数据资源目录。
3. 公共管理和服务机构新建业务系统，要同步规划编制有关公共数据资源目录。
4. 全区各级公共数据资源目录应按照统一的技术标准，在本级公共数据资源共享交换平台发布。
5. 公共数据资源共享交换平台应提供目录更新、维护、调用等技术接口，供各部门调用。
6. 按照数据类别或主题形成数据资源清单与目录，确保目录发布的操作通过共享交换服务方鉴别身份并取得授权才可进行。
7. 明确定义公共数据资源目录对应数据资源的安全分级与共享类型。
8. 对公共数据资源目录发布进行审核，检查资源目录项的规范性、准确性。
9. 对目录共享类型变更、目录迁移等操作进行授权审计。
10. 在资源目录信息发布过程中，如提交、同步、展示等环节，保证信息的保密性和一致性。
11. 明确公共数据资源共享方式与内容，遵循最小化策略，仅提供业务开展明确所需的数据内容及规模；
12. 检查共享公共数据资源发布信息与已有目录的关联关系，防止发布目录外的共享公共数据资源。\*
13. 明确规定共享公共数据资源的安全级别，建立相应的安全策略(如脱敏、加密等) 确保敏感数据在共享过程中的保密性。
14. 对共享公共数据资源发布进行审核，检查发布项的规范性、安全策略合规性。
15. 建立公共数据资源共享方式的变更与注销机制，及时通知使用者进行调整，防止影响相关业务系统。
16. 对共享公共数据资源发布过程进行详细记录，包括发布日期和时间、发布人、审批人、发布资源详细内容等。
17. 在共享公共数据资源发布信息传递过程中，如提交、同步、展示等环节，保证信息的保密性和一致性。

5.5 数据分类分级

基于政策法规及公共数据共享和安全需求，确定组织机构内部的数据分类分级方法，对公共数据进行分类分级标识。

公共管理和服务机构应：

1. 设立负责数据安全分类分级工作的管理岗位和人员，由该岗位和人员负责定义组织整体的数据分类分级的安全原则。
2. 明确数据分类分级原则、方法和操作指南。
3. 对组织的数据进行分类分级标识和管理。
4. 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。
5. 明确数据分类分级变更审批流程和机制，通过该流程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。
6. 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。
7. 确保负责该项工作的人员了解数据分类分级的合规要求，能够识别敏感数据。

5.6 元数据管理

建立组织机构的元数据管理体系，实现对组织机构内公共元数据的有效集中管理。

公共管理和服务机构应：

1. 设立组织层面的元数据管理的岗位和人员，由该岗位和人员统一负责建立组织内部元数据语义规则、管理要求和技术工具。
2. 明确元数据语义统一格式和管理规则，如数据格式、数据域、字段类型、表结构、逻辑存储和物理存储结构及管理方式。
3. 明确元数据安全管理要求，如口令策略、权限列表、授权策略。
4. 确保元数据管理工具支持数据表的导航和搜索，提供表血缘关系、字段信息、使用说明、其它关联信息，方便用户使用数据表。
5. 建立元数据访问控制策略和审计机制，确保元数据操作的追溯。
6. 确保负责该项工作的人员了解元数据管理的理论基础，理解组织的元数据管理的业务需求。

5.7 敏感数据保护

公共数据主管机构应建立针对敏感数据的保护机制，防止敏感数据外泄或滥用。

公共数据管理部门应：

1. 设立负责鉴别、管理、保护敏感数据的岗位或人员。
2. 确定敏感数据范围，明确敏感数据安全防护要求。
3. 建立部门间敏感数据防护意识，确保组织内所有人员对敏感数据具有统一、清晰的认识。
4. 提出敏感数据安全防护要求，对敏感数据进行脱敏、权限管控等必要的安全防护，保证数据不被滥用或外泄。
5. 确保负责该项工作的人员具备敏感数据鉴别和防护的能力，熟悉敏感数据保护技术和相关机制。

5.8 终端数据安全

基于组织机构对终端层面的数据保护要求，针对组织机构内部的工作终端采取相应的技术和管理方案。

公共管理和服务机构应：

1. 设立统一的终端数据安全管理岗位和人员。
2. 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漏管理要求等。
3. 确保打印输出设备采用身份鉴别、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。
4. 确保组织内入网的终端设备均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，并将终端设备纳入组织整体的访问控制体系中。
5. 部署终端数据防泄漏方案，通过技术工具对终端设备上数据以及数据的操作进行风险监控。
6. 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）。
7. 确保负责该项工作的人员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。

5.9 监控与审计

针对数据生命周期各阶段（数据采集、数据传输、数据存储、数据处理、数据交换、数据退役）开展安全监控和审计，以保证对数据的访问和操作均得到有效的监控和审计，实现对数据生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等安全风险的防控。

公共管理和服务机构应：

1. 设立负责对数据生存周期各阶段的数据访问和操作的安全风险进行监控和审计的岗位和人员，该岗位和人员属于组织风险管理架构的一部分，遵循风险管理整体的职能设置。
2. 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。
3. 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。
4. 定期对组织内部员工数据操作行为进行人工审计。
5. 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。
6. 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，将高敏感数据及特权账户对数据的访问和操作都纳入重点的监控范围。
7. 部署必要的数据防泄漏实时监控技术手段，监控及报告个人信息、重要数据等的外发行为。
8. 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。
9. 确保负责该项工作的人员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。

5.10 鉴别与访问控制

通过基于组织机构的数据安全需求和合规性要求，建立身份鉴别和数据访问控制机制，防止对数据的未授权访问风险。

公共管理和服务机构应：

1. 设立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的岗位和人员。
2. 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。
3. 按最少够用、职权分离等原则，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
4. 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。
5. 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。
6. 对外包人员和实习生的数据访问权限进行严格控制。
7. 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。
8. 建立组织统一的权限管理系统，支持组织主要应用接入，对人员访问数据资源进行访问控制和权限管理。
9. 采用技术手段实现身份鉴别和权限管理的联动控制。
10. 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。
11. 确保访问控制的粒度达到主体为用户级，客体为系统、文件、数据库表级或字段。
12. 确保负责该项工作的人员熟悉相关的数据访问控制的技术知识，并能够根据组织数据安全管理制度对数据权限进行审批管理。

5.11 需求分析

通过建立针对组织机构业务的数据安全需求分析体系，分析组织机构内数据业务的安全需求。

公共管理和服务机构应：

1. 设立负责数据安全需求分析的岗位和人员，由该岗位和人员负责对数据业务设计、开发等阶段开展数据安全需求分析工作，确保安全需求的有效制定和规范化表达。
2. 明确数据安全需求分析的制定流程和评审机制，明确安全需求文档内容要求。
3. 依据国家法律、法规、标准等要求，分析数据安全合规性需求。
4. 结合机构战略规划、数据服务业务目标和业务特点，明确数据服务安全需求和安全规划实施的优先级。
5. 识别数据服务面临的威胁和自身脆弱性，分析数据安全风险和应对措施需求。
6. 建立承载数据业务的安全需求分析系统，该系统记录所有的数据业务的需求分析的申请、需求分析以及相关安全方案，以保证对所有的数据业务的安全需求分析过程的有效追溯。
7. 确保负责该项工作的人员具有需求分析挖掘能力，对组织的数据安全管理的业务有充分的理解，各业务的需求分析人员对数据安全需求分析标准有一致性理解。

5.12 数据供应链安全

通过建立组织机构的数据供应链和供应商管理机制，防范组织机构上下游的数据供应过程中的安全风险。

公共管理和服务机构应：

1. 设置组织整体的数据供应链安全管理岗位和人员，由该岗位和人员负责制定整体的数据供应链管理要求和解决方案。
2. 明确数据供应链安全管理规范，定义数据供应链安全目标、原则和范围，明确数据供应链的责任部门和人员、数据供应链上下游的责任和义务以及组织内部的审核原则。
3. 通过合作协议方式明确数据供应链中，数据的使用目的、供应方式、保密约定、安全责任义务等。
4. 应明确针对数据供应商的数据安全能力评估规范，根据该规范对数据供应商的数据安全能力进行评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中。
5. 应建立组织整体的数据供应链库，用于管理数据供应链目录和相关数据源数据字典，便于及时查看并更新组织上下游数据供应链的整体情况，并用于事后追踪分析数据供应链上下游合规情况。
6. 建立供应商安全管理规范，定义供应商安全管理的目标、原则和范围，明确责任部门和人员、数据供应链上下游的责任和义务以及组织机构内部的审核原则。
7. 通过合作协议方式明确数据链中数据的使用目的、供应方式、保密约定、安全责任义务等。
8. 制定针对数据供应商的数据安全能力评估规范，根据该规范对数据供应商的数据安全能力进行评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中。
9. 采取技术措施和管理手段，确保数据供应链上下游对数据交换、使用符合法律法规，数据供应链相关数据服务真实可用。
10. 建立组织机构数据供应链目录和相关数据源数据字典。
11. 负责该项过程的人员应了解组织机构上下游数据供应链的整体情况，熟悉供应链安全方面的法规和标准，并具备推进供应链管理方案落地的能力。

5.13 安全事件应急

建立针对数据的安全事件应急响应体系，对各类安全事件进行及时响应和处置。

公共管理和服务机构应：

1. 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，由该岗位和人员牵头制定数据安全应急响应工作要求、处置流程，编制应急预案，规划实施应急演练工作。
2. 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。
3. 明确数据安全事件应急预案，定期开展应急演练活动。
4. 确保组织的数据安全事件应急响应机制符合国家有关主管部门的政策文件要求。
5. 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。
6. 确保负责该项工作的人员具备安全事件的判断能力，熟悉安全事件应急响应措施。
7. 安全监管

公共数据主管机构建立针对数据安全的监管体系，确立对各类数据安全管理的监管要求。

公共数据管理部门：

1. 对公共数据安全管理实行统一领导和分级管理，按照“谁主管谁负责，谁使用谁负责”的原则，落实公共数据主管部门和相关部门的安全责任。数据流转中涉及的相关方均有数据安全保护职责，如在数据共享交换环节，数据提供方、接收方均负有数据安全职责。
2. 安全监管可由公共数据主管、监管部门按职能共同负责，承担对公共数据资源共享交换平台接入和输出边界的安全态势监管、内容安全监管、失泄密监管。
3. 应建立公共数据安全事件通报预警与应急响应机制。
4. 公共数据主管部门可通过随机抽查、定期检查和电子督查等方式，对公共数据资源的编目、挂接、共享、应用等情况进行日常监督，对于发现的问题及时落实整改。
5. 建立健全公共数据安全工作监督检查机制，明确监督检查的牵头部门、责任分工、内容、重点、目标、方式和标准。
6. 公共数据主管部门组织制定公共数据安全管理考核方案，可委托第三方机构，围绕公共数据安全能力、共享交换程度、应用支撑能力等方面开展评估并公开结果。
7. 如被采集人认为公共管理和服务机构采集、开放的数据存在错误、遗漏等情形，或者侵犯其个人隐私、商业秘密等合法权益的，可向公共数据主管或监管部门提出异议。
8. 对自治区公共管理和服务机构，组织开展相关数据安全法律法规、标准规范和知识技能的宣传培训。
9. 指导公共数据资源分类分级、个人信息保护、数据安全评估等相关工作。
10. 监督组织机构落实国家、自治区法律法规、标准规范的情况，特别是有强制性要求的法律法规、标准规范，如等级保护等。
11. 数据采集安全

7.1 数据采集安全管理

在采集公共数据的过程中，需明确采集数据的目的和用途，确保数据源的真实性、有效性和最少够用等原则，并规范数据采集的渠道、数据的格式以及相关的流程和方式，从而保证数据采集的合规性、正当性和执行上的一致性。

公共管理和服务机构应：

1. 设立数据采集安全管理的岗位和人员，由该岗位和人员负责制定相关的公共数据采集安全管理的制度，推动相关要求、流程的落地，并对具体业务或项目的风险评估提供咨询和支持。
2. 遵循合法、必要、适度原则，按照法定范围和程序采集公共数据。
3. 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。
4. 可采取直接采集、委托第三方机构采集或者协商的方式采集公共数据，也可通过业务系统、监测、测量、录音、录像等方式产生有关数据。
5. 确保通过业务系统、监测、测量、录音、录像等方式产生公共数据资源的过程中，遵守保护国家秘密、商业秘密和个人隐私的相关规定。
6. 确保公共管理和服务机构因履职需要，采集法律、法规未作规定的数据时，取得被采集人同意，如采集人主动填报公共数据，视为取得采集人同意。
7. 明确组织的数据采集原则，定义业务的数据采集流程和方法。
8. 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。
9. 明确数据采集范围、数量和频度，确保不收集与提供服务无关的个人信息和重要数据。
10. 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。
11. 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，采取技术手段保证数据采集过程中个人信息和重要数据不被泄漏。
12. 依据统一的数据采集流程建设数据采集相关的工具，保证组织数据采集流程实现的一致性，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。
13. 确保负责该项工作的人员充分理解数据采集的法律要求、安全和业务需求，根据组织的业务提出针对性的解决方案。

7.2 数据源鉴别及记录

对公共数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造。

公共管理和服务机构应：

1. 设立负责数据源鉴别和记录的岗位和人员。
2. 明确数据源管理制度，对采集的数据源进行鉴别和记录。
3. 采取技术手段对外部收集的数据和数据源进行识别和记录。
4. 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. 确保负责该项工作的人员理解数据源鉴别标准和组织内部的数据采集业务，并结合实际情况执行标准要求。
6. 制定数据源管理的制度规范，定义数据溯源安全策略和溯源数据格式等规范，明确提出对公共数据的数据源进行鉴别和记录的要求。
7. 通过身份鉴别、数据源认证等安全机制确保数据来源的真实性。

7.3 数据质量管理

建立公共数据质量管理体系，保证对数据采集过程中收集/产生的数据的准确性、一致性和完整性。

公共管理和服务机构应：

1. 设立福州数据质量管理岗位和人员，由该岗位和人员负责制定统一的数据质量管理要求，明确对数据质量进行管理和监控的责任部门或人员。
2. 明确数据质量管理相关要求，包含数据格式要求、数据完整性要求、数据源质量评价标准等。
3. 明确数据采集过程中的质量监控规则，明确数据质量监控范围及监控方式。
4. 明确公共数据质量管理规范，及对异常事件处理的流程和操作规范。
5. 明确数据清洗、转换和加载操作相关的安全管理规范、执行的规则和方法、相关人员权限、完整性和一致性要求等。
6. 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。
7. 确保负责该项工作的人员理解数据采集阶段的数据质量控制要素，能够基于组织的业务特点开展数据质量评估工作。
8. 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，确有错误的，应予以更正。
9. 数据传输安全

8.1 数据传输加密

根据组织内部和外部的数据传输要求，采用适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄漏。

公共管理和服务机构应：

1. 设立负责数据加密、密钥管理的人员，由该岗位和人员确定加密原则和技术工作，指导技术团队负责实现具体场景下的数据传输加密。
2. 明确公共数据传输安全管理规范、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。
3. 建立密钥管理安全规范，明确密钥生成、分发、存取、更新、备份和销毁的流程和要求。
4. 明确对数据传输安全策略的变更进行审核的技术方案。
5. 有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。
6. 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。
7. 采取技术手段对公共数据传输通道两端进行主体身份鉴别和认证。
8. 采取技术手段实现公共数据传输加密，包括数据传输通道加密和数据传输内容加密。
9. 采取技术手段实现对密钥的全生命周期（生成、存储、使用、分发、更新、销毁等）的安全管理，并提供数据的加密解密、签名验签等功能。
10. 确保负责该项工作的人员熟悉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，能够基于具体的业务选择合适的数据传输安全管理方式和合适的加密技术。

8.2 网络可用性管理

通过网络基础设施及网络层数据防泄漏设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。

公共管理和服务机构应：

1. 设立负责网络可用性管理的岗位和人员。
2. 制定组织的网络可用性管理指标，包括可用性的概率数值、故障时间/ 频率/统计业务单元等；基于可用性管理指标，建立网络服务配置方案和宕机替代方案等。
3. 对关键的网络传输链路、网络设备节点实行冗余建设。
4. 部署相关设备对网络可用性及数据泄漏风险进行防范，如负载均衡、防入侵攻击、数据防泄漏检测与防护等设备。
5. 确保负责该项工作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，能够根据不同业务对网络性能需求制定有效的可用性安全防护方案。
6. 数据存储安全

9.1 存储媒介安全

针对组织内需要对公共数据存储媒介进行访问和使用的场景，提供有效的技术和管理手段，防止不当使用而可能引发的数据泄漏风险。存储媒介包括终端设备及网络存储。

公共管理和服务机构应：

1. 设立统一负责存储媒介安全管理的岗位和人员。
2. 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。
3. 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。
4. 建立存储媒介资产标识，明确存储媒介存储的数据。
5. 对存储媒介进行常规和随机检查，确保存储媒介的使用符合机构公布的关于存储媒介使用的制度。
6. 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、错误或损坏情况，对超过安全阈值的存储媒介进行预警。
7. 对存储媒介访问和使用行为进行记录和审计。
8. 确保负责该项工作的人员熟悉存储媒介安全管理的相关合规要求，熟悉不同存储媒介访问和使用的差异性。

9.2 逻辑存储安全

基于公共数据业务特性和数据存储安全要求，建立针对公共数据库和逻辑存储架构的有效安全控制。

公共管理和服务机构应：

1. 设立组织内统一负责数据逻辑存储安全管理的岗位和人员，由该岗位和人员明确整体的数据逻辑存储系统安全管理要求，并推进相关要求的实施。
2. 设立各数据逻辑存储系统的安全管理员，负责执行数据逻辑存储系统、存储设备的安全管理和运维工作。
3. 明确数据逻辑存储管理安全规范和配置规则，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。
4. 确保内部的数据存储系统在上线前应遵循统一的配置要求进行有效的安全配置，对使用的外部数据存储系统也进行有效的安全配置。
5. 明确数据逻辑存储隔离授权与操作要求，确保具备多用户数据存储安全隔离能力。
6. 提供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，保证符合安全基线要求。
7. 利用技术工具监测逻辑存储系统的数据使用规范性，确保数据存储符合组织的相关安全要求。
8. 具备对个人信息、重要数据等敏感数据的加密存储能力。
9. 对敏感公共数据采用符合国家相关规定的数据加密方式与密码算法进行加密存储保护。
10. 确保负责该项工作的人员应熟悉数据存储系统架构，并能够分析出数据存储面临的安全风险，从而能够保证对各类存储系统的有效安全防护。

9.3 数据备份和恢复

通过对公共数据定期的备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。

公共管理和服务机构应：

1. 明确负责数据备份和恢复管理工作的岗位和人员，由该岗位和人员负责建立相应的制度流程并部署相关的安全措施。
2. 明确数据备份与恢复的管理制度，以满足数据服务可靠性、可用性等安全目标。
3. 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。
4. 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，。
5. 依据数据生存周期和业务规范，建立数据生命周期各阶段数据归档的操作流程。
6. 明确归档数据的压缩或加密要求。
7. 明确对归档数据的安全管控措施，非授权用户不能访问归档数据。
8. 识别组织适用的合规要求，按监管部门的要求对相关数据予以记录和保存。
9. 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。
10. 明确过期存储数据的安全保护机制，对超出有效期的存储数据应具备再次获取数据控制者授权的能力。
11. 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。
12. 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。
13. 定期采取必要的技术措施查验备份和归档数据的完整性和可用性。
14. 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、无法恢复或无法识别到个人，并告知数据控制者和数据使用者。
15. 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。
16. 确保存储架构具备跨机柜或跨机房容错部署的能力。
17. 确保负责该项工作的人员了解数据备份媒体的性能和相关数据的业务特性，能够确定有效的数据备份和恢复机制。
18. 确保负责该项工作的人员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。
19. 数据使用安全

10.1数据脱敏

根据公共数据相关法律法规、标准的要求以及业务需求，对敏感公共数据进行脱敏处理，保证数据可用性和安全性的平衡。

公共管理和服务机构应：

1. 设立负责数据脱敏的岗位和人员，由该岗位和人员制定数据脱敏的原则和方法，并提供相关技术支持。
2. 在数据权限的申请阶段，有相关人员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。
3. 明确组织的数据脱敏规范，明确数据脱敏的规则、脱敏方法和使用限制等。
4. 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。
5. 供统一的数据脱敏工具，实现数据脱敏工具与数据权限管理系统的联动，以及数据使用前的静态脱敏。
6. 提供面向不同数据类型的脱敏方案，可基于场景需求自定义脱敏规则。
7. 确保数据脱敏后保留原始数据格式和特定属性，满足开发与测试需求。
8. 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。
9. 确保负责该项工作的人员熟悉常规的数据脱敏技术，能够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。
10. 确保负责该项工作的人员具备对数据脱敏的技术方案定制化的能力，能够基于组织内部各级别的数据建立有效的数据脱敏方案。

10.2 数据分析安全

通过对公共数据整合分析利用过程采取适当的安全措施，防止公共数据挖掘、分析过程中有价值信息和个人隐私泄露的安全风险。

公共管理和服务机构应：

1. 设立负责数据分析安全的岗位和人员，由该岗位和人员负责制定数据分析安全原则、提供相应技术支持。
2. 明确数据处理与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。
3. 明确数据分析安全审核流程，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。
4. 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对数据的权限范围。
5. 明确数据分析结果输出和使用的安全审核、合规评估和授权流程，防止数据分析结果输出造成安全风险。
6. 在针对个人信息的数据分析中，采用多种技术手段以降低数据分析过程中的隐私泄漏风险，如差分隐私保护、K匿名等。
7. 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。
8. 提供组织统一的数据处理与分析系统，并能够呈现数据处理前后数据间的映射关系。
9. 确保负责该项工作的人员能够基于合规性要求、相关标准，对数据安全分析中所可能引发的数据聚合的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。

10.3 数据正当使用

基于国家相关法律法规对公共数据使用的要求，建立公共数据使用过程的责任机制、评估机制，保护国家秘密、商业秘密和个人隐私，防止公共数据资源被用于不正当目的。

公共管理和服务机构应：

1. 设立负责对数据正当使用管理、评估和风险控制的岗位或人员。
2. 明确数据使用的评估制度，使用个人信息和重要数据前，先进行安全影响评估，保证满足国家合规要求后，才允许使用。
3. 避免数据使用时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，不得超出与收集数据时所声明的目的和范围。
4. 明确数据使用正当性的制度，保证数据使用在声明的目的和范围内。
5. 依据数据国家合规要求，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。
6. 完整记录数据使用过程的操作日志，以备识别潜在违约使用者的责任。
7. 确保负责该项工作的人员能够按照最小够用等原则管理权限，并具备对数据正当使用相关风险的分析和跟进能力。

10.4 数据处理环境安全

为组织内部的公共数据处理环境建立安全保护机制，提供统一的数据计算、开发平台，确保公共数据处理的过程中有完整的安全控制管理和技术支持。

公共管理和服务机构应：

1. 明确业务团队负责数据处理环境安全管理的岗位和人员。
2. 确保在数据处理环境的系统设计、开发和运维阶段制定相应的安全控制措施，实现对安全风险的管理。
3. 明确对数据处理环境的安全管理要求。
4. 基于数据处理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漏等方面进行安全要求和控制。
5. 明确适合数据处理环境的数据加解密处理策略和密钥管理要求。
6. 确保大数据平台具备分布式处理过程中数据文件鉴别和访问用户身份认证的策略，保障分布式处理数据文件的可访问性。
7. 实现数据处理系统与数据权限管理系统的联动机制，确保用户在使用数据系统前已获得授权。
8. 确保基于数据处理系统的多租户的特性，对不同的租户保证其在该系统中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制。
9. 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。
10. 确保大数据平台具备分布式处理节点间可信连接策略和规范，采用节点认证等机制确保节点接入的真实性。
11. 确保负责该项工作的人员了解在数据环境下的数据处理系统的主要安全风险，并能够在相关的系统设计、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。

10.5 数据导入导出安全

通过对数据导入、导出过程中对数据的安全性进行管理，防止公共数据导入导出过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的公共数据泄漏风险。

公共管理和服务机构应：

1. 设立负责数据导入导出安全管理岗位和人员，由岗位和人员负责制定规则和提供技术能力，推动在组织机构内业务场景落地执行。
2. 依据数据分类分级要求，建立数据导入导出安全策略，如授权和访问控制策略、脱敏策略、加密策略等。
3. 按照数据提供方对共享数据的分级分类要求，建立相应的授权和访问控制机制，标记数据资产的责任主体。
4. 建立数据导出安全评估和授权审批流程，评估数据导出的安全风险，并对大量或敏感数据导出进行授权审批。
5. 按照数据导入导出安全策略，将敏感数据脱敏后再导出。
6. 具有对数据导入过程的保护和回退机制，保证获取过程中产生问题时能有效还原和恢复数据。
7. 具有数据自动加载的故障恢复能力。
8. 在数据导入时检验数据的质量，包括对数据格式和接口提出统一要求，并对获取数据是否满足要求做出认定。
9. 建立针对导出介质的标识规范，明确介质的命名规则、标识属性等重要信息，定期验证导出数据的完整性和可用性。
10. 制定导入导出审计策略和日志管理规范，并保存导入导出过程中的异常数据处理记录。
11. 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。
12. 对数据导入导出终端、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。
13. 采取数据加密、访问控制等技术手段，保障数据在传输中的保密性、完整性和可用性。
14. 在导入导出完成后，清除数据导入导出通道缓存的数据，保证导入导出过程中涉及的数据不被恶意恢复。
15. 确保负责数据导入导出安全工作的人员充分理解组织机构的数据导入导出策略，并根据数据导入导出的业务场景执行相应的风险评估，提出实际的解决方案。
16. 数据交换安全

11.1数据共享安全

通过对公共数据共享交换过程的安全控制，降低数据共享交换场景下的安全风险。

公共服务和管理机构应：

1. 设立负责数据共享交换安全管理的岗位和人员，由该岗位和人员负责相关原则和技术能力的提供，推广相关要求在相关业务的落地执行。
2. 根据法定职责，明确本机构能够向其他单位共享的公共数据责任清单，根据履职需求形成需要其他单位予以共享的公共数据需求清单，将法律、法规、规章明确规定不能共享的公共数据列入共享负面清单。
3. 明确数据共享的原则和安全规范，明确数据共享内容、范围、、管控措施、涉及机构或部门相关用户职责和权限。
4. 明确数据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。
5. 明确数据共享审计规程和审计日志管理要求，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。
6. 在使用外部第三方的SDK/组件/源码前进行安全评估，确保第三方获取的数据符合组织机构的数据安全要求。采取措施确保个人信息在委托处理、共享、转让等对外提供场景的安全合规，如数据脱敏、数据加密、安全通道、共享交换区域等。
7. 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。
8. 明确共享数据格式规范，如提供机器可读的格式规范。
9. 确保负责该项工作的人员应能够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。

11.2 数据开放安全

在对外部组织进行公共数据发布的过程中，通过对发布数据的格式、适用范围、发布者与使用者权利和义务执行必要控制，实现公共数据发布过程中数据的安全可控与合规。

公共服务和管理机构应：

1. 设立负责数据开放安全的岗位和人员，由该岗位和人员负责组织的数据公开发布信息，对数据发布人员进行安全培训。
2. 明确数据开放的审核制度，严格审核数据开放合规要求。
3. 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。
4. 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。
5. 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。
6. 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。
7. 确保负责数据发布安全管理工作的人员充分理解数据安全发布的制度和流程，通过岗位能力评估，确保其能够根据实际发布要求建立相应的应急方案。

11.3 数据接口安全

通过建立公共服务数据接口的安全管理机制，防范组织机构在数据接口调用过程中的安全风险。

公共服务和管理机构应：

1. 设立统一负责数据接口安全管理的岗位和人员，由该岗位人员负责制定整体的规则并推广相关流程的推行。
2. 明确数据接口安全控制策略，规定使用数据接口的安全限制和安全控制措施，如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议、异常流量管控和熔断控制等。
3. 明确数据接口安全要求，包括接口名称、接口参数等。
4. 与数据接口调用方签署了合作协议，明确数据的使用目的、供应方式、保密约定、数据安全责任等。
5. 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。
6. 具备数据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。
7. 对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施。
8. 确保负责数据接口安全工作的人员充分理解数据接口调用业务的使用场景，具备充分的数据接口调用的安全意识、技术能力和风险控制能力
9. 数据退役安全

12.1 数据退役处置

通过建立针对公共数据的归档、转移、删除、净化机制，实现公共数据退役，防止因对存储媒介中的数据进行恢复而导致的公共数据泄漏风险。

公共服务和管理机构应：

1. 设立统一负责公共数据退役管理的岗位和人员，由该岗位和人员制定公共数据退役处置规范，明确公共数据转移和归档要求，推动相关要求在业务部门落地实施。
2. 建立组织的数据归档流程，明确归档安全要求，对归档数据进行审批、记录，确保所有归档过程可控、可溯源、可审计。
3. 建立明确的数据转移流程，明确数据转移安全要求，数据在组织内部或组织间转移时，应进行数据转移的安全风险评估。
4. 记录转移过程和转移的数据情况，保证数据转移过程的安全可靠和可用性，确保转移数据的一致性、完整性。
5. 可单独采用电子归档形式，按国家和自治区有关规定对公共数据资源进行归档和登记备份。
6. 建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问。
7. 建立归档数据的安全策略和管控措施，确保非授权用户不能访问归档数据。
8. 依照数据分类分级建立数据退役策略和管理制度，明确数据退役的场景、退役对象、退役方式和退役要求。
9. 建立规范的数据退役流程和审批机制，设置退役过程的相关监督角色，监督操作过程，并对审批和退役过程进行记录控制。
10. 按国家相关法律和标准销毁个人信息、重要数据等敏感数据。
11. 针对网络存储数据，建立硬销毁和软销毁的数据退役方法和技术，如基于安全策略、基于分布式杂凑算法等网络数据分布式存储的退役策略与机制。
12. 配置必要的数据退役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。
13. 确保负责数据退役安全工作的人员应熟悉数据销毁的相关合规要求，能够主动根据政策变化和技术发展更新相关知识和技能。

12.2 存储介质销毁处置

针对损坏或报废的存储介质，建立对介质安全销毁的管理和技术手段，防止因介质丢失、被窃或未授权的物理访问而导致介质中的数据面临泄漏的安全风险。

公共服务和管理机构应：

1. 设立统一负责存储介质销毁管理的岗位和人员，由该岗位和人员制定组织的介质销毁管理制度，推动相关内容在业务团队实施落地。
2. 明确存储介质销毁处理策略、管理制度和机制，明确销毁对象和流程。
3. 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存储介质的销毁方法。
4. 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、交接等存储介质销毁过程进行监控。
5. 按照国家相关法律和标准销毁存储介质，加强对介质销毁人员监管。
6. 提供统一的存储介质销毁工具，包括但不限于物理销毁、消磁设备等工具，能够实现对各类介质的有效销毁。
7. 针对闪存盘、硬盘、磁带、光盘等存储介质数据，建立硬销毁和软销毁的数据退役方法和技术。
8. 确保负责该项工作的人员应能够依据数据退役的整体需求明确应使用的媒体介质工具。

参考文献

1. GB/T 35273-2017 信息安全技术 个人信息安全规范
2. GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_