ICS 35.240
CCS L 70

DB11

北　京　市　地　方　标　准

DB11/T 2049—2022

政务大数据安全技术框架

Technical framework of government big data security

2022-12-27 发布　　2023-04-01 实施

北京市市场监督管理局　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。

本文件由北京市经济和信息化局提出并归口。

本文件由北京市经济和信息化局组织实施。

本文件起草单位：北京市大数据中心、中电长城网际系统应用有限公司、北京信息安全测评中心、联通数字科技有限公司、北京数字认证股份有限公司、北京天融信网络安全技术有限公司、厦门市美亚柏科信息股份有限公司、数据堂（北京）科技股份有限公司、北京云集至科技有限公司、北京启明星辰信息安全技术有限公司、京信数据科技有限公司。

本文件主要起草人：赵章界、赵莹、张琳、徐海琛、窦腾飞、王竹欣、刘国伟、高磊、宁振宇、张兴、马洪军、李媛、蓝宇娜、李向锋、李建彬、王斌、齐红威、张海涛、周瑞群、王延康、刘倩、宋劲松。

政务大数据安全技术框架

1 范围

本文件提出了政务大数据安全技术框架，规定了政务大数据域安全要求、政务大数据域间协同安全要求以及基础设施安全要求等。

本文件适用于指导政务部门以及参与政务大数据处理活动的相关组织开展政务大数据安全技术体系规划、建设、监督与管理。

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 20269 信息技术 大数据 大数据系统基本要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

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

GB/T 35295 信息技术 大数据 术语

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 38664.2 信息技术 大数据 政务数据开放共享 第2部分：基本要求

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

DB11/T 1918 政务数据分级与安全保护规范

3 术语和定义

GB/T 35295界定的以及下列术语和定义适用于本文件。

3.1

大数据 big data

具有体量巨大、来源多样、生成极快且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[来源：GB/T 35295—2017,2.1.1]

3.2

政务大数据 government big data

政务部门在履行职责过程中制作或获取的，以电子化形式记录、保存的大数据。

3.3

政务大数据域 government big data domain

在政务大数据处理活动中，遵从共同安全策略的资源和资产的集合。

注：数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

3.4

政务大数据参与方 participant of government big data

参与政务大数据处理活动的主体。

3.5

政务大数据基础设施 infrastructure for government big data

为政务大数据处理活动提供算力、存储、网络、安全等服务的信息基础设施。

4 政务大数据安全技术框架的构成

4.1 技术框架

政务大数据安全技术框架如图1所示，包括政务大数据域、政务大数据基础设施、政务大数据参与方。政务大数据处理中，其资源和资产按照所遵循安全策略的不同分为数据生产域、数据加工域、数据共享域、数据开放域、数据运营域等政务大数据域；政务大数据基础设施为各个政务大数据域的数据处理活动提供了基础的、统一的资源服务和安全服务；政务大数据参与方包含了参与各个政务大数据域的数据处理活动以及政务大数据基础设施建设、管理、运营的相关方。

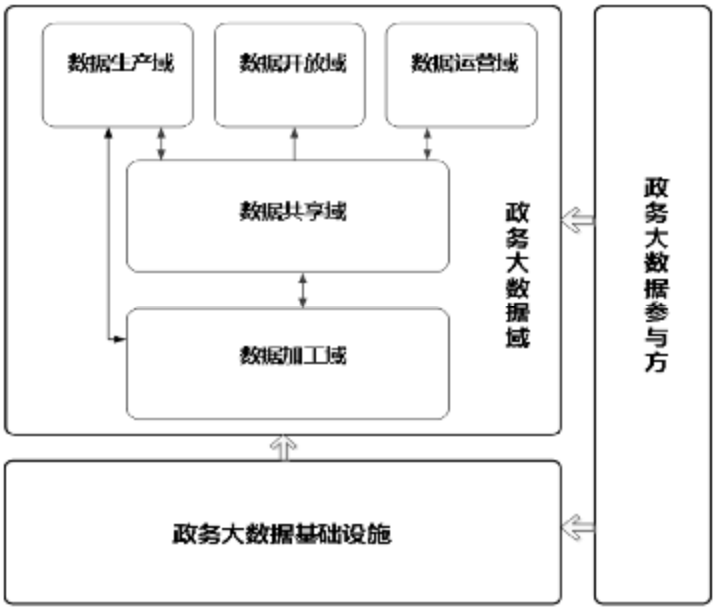

图1 政务大数据安全技术框架

4.2 政务大数据域

4.2.1 政务大数据域类型

综合考虑政务大数据的流动环节和落地场景，政务大数据域包括：数据生产域、数据加工域、数据共享域、数据开放域、数据运营域五类，各政务大数据域的主要功能如表1所示，各政务大数据域所包含的资源和资产示例见附录A。

表1 政务大数据域主要功能

名称	主要功能
数据生产域	对政务大数据进行收集、生产和使用
数据加工域	对政务大数据进行加工以形成政务大数据资产
数据共享域	政务部门之间或在政务部门内部提供或获取政务大数据
数据开放域	面向社会提供政务大数据
数据运营域	面向社会特定群体提供政务大数据，以开展数据运营服务

4.2.2 政务大数据域间协同关系

4.2.2.1 政务大数据在同一政务部门内的政务大数据域之间流动的情况，如图2所示。

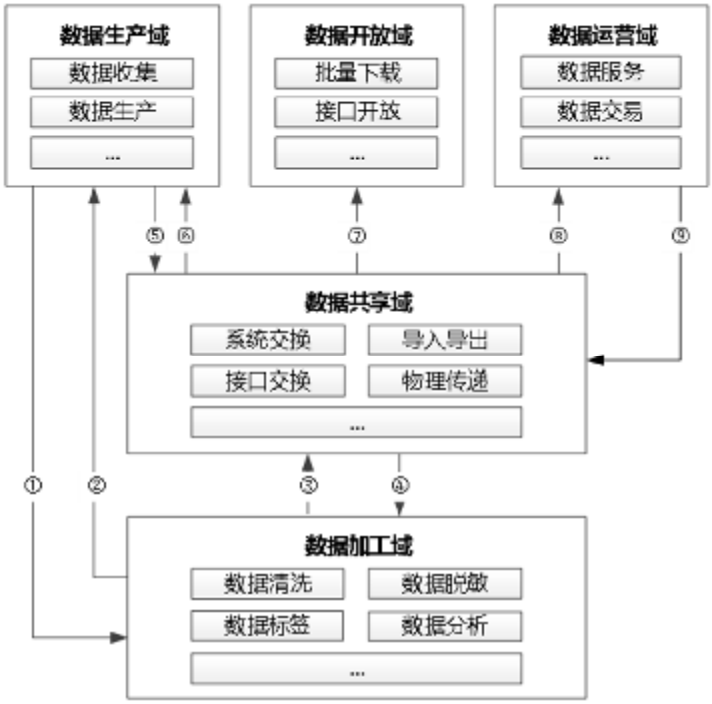

图2 政务大数据域间流动图

标引序号说明：

1—数据生产域收集、生产的数据，进入到数据加工域进行加工；

2—经数据加工域加工后的数据，进入到数据生产域进行使用；

3—经数据加工域加工后的数据，进入数据共享域进行共享；

4—数据共享域中的数据，进入数据加工域进行加工；

5—数据生产域收集、生产的数据，进入共享域进行共享；

6—数据共享域中的数据，进入数据生产域进行使用；

7—数据共享域中的数据，进入数据开放域面向社会进行开放；

8—数据共享域中的数据，进入数据运营域以开展数据运营；

9—数据运营域产生新数据，进入数据共享域以进行共享。

4.2.2.2 政务大数据在不同政务部门间通过数据共享域实现跨组织交换，如图3所示。

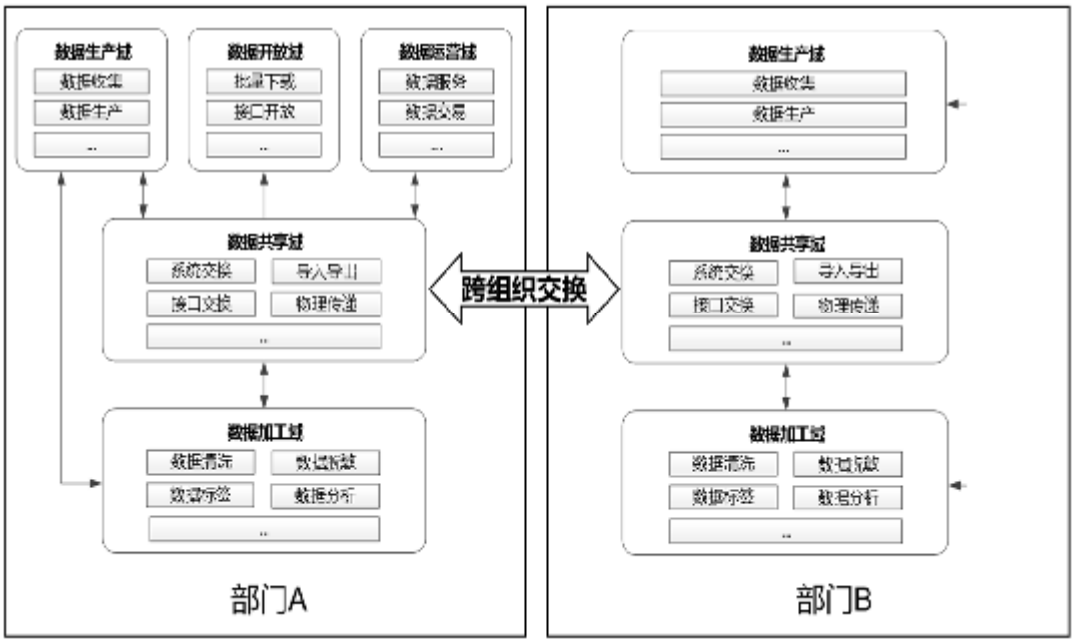

图3 政务大数据跨组织流动图

4.2.2.3 不同政务大数据域之间进行数据流动时，应按照协议或者约定进行安全协作联动和互相配合，即域间安全协同。主要的域间协同关系见表2。

表2 政务大数据域间协同关系

	数据生产域	数据加工域	数据共享域	数据开放域	数据运营域
数据生产域	/	●	●	/	/
数据加工域	●	/	●	/	/
数据共享域	●	●	●	●	●
数据开放域	/	/	●	/	/
数据运营域	/	/	●	/	/
注：“●”代表域间需要直接协同，“/”代表域间不需要直接协同。					

4.3 政务大数据基础设施

政务大数据基础设施包括基础资源平台和基础安全平台等。基础资源平台为政务大数据处理活动提供统一的算力、存储和网络等基础资源服务；基础安全平台为政务大数据处理活动提供统一的身份认证、密码服务、数据监测溯源等基础安全保障，如图4所示。

图4 政务大数据基础设施图

4.4 政务大数据参与方

4.4.1 政务大数据处理维度的参与方

根据参与方在政务大数据处理过程中的角色类型，政务大数据参与方可分为数据控制者、数据生产者、数据加工者、数据运营者、数据使用者和平台运营者六类，各参与方的定义见表3，各参与方与政务大数据域、政务大数据基础设施的关系见表4，各参与方示例见附录A。

表3 政务大数据处理维度的参与方

角色	定义
数据控制者	有权决定数据处理目的、方式，对数据进行管控的组织、个人
数据生产者	收集、生产数据的组织、个人
数据加工者	清洗、加工数据的组织、个人
数据运营者	开发、提供数据服务的组织
数据使用者	使用、消费数据的组织、个人
平台运营者	处理政务数据的信息系统或政务大数据基础设施的所有者、管理者和服务提供者

表4 政务大数据处理维度的参与方与政务大数据域及基础设施的关系

		数据控制者	数据生产者	数据加工者	数据运营者	数据使用者	平台运营者
政务大数据域	数据生产域	●	●	/	/	●	●
	数据加工域	●	/	●	/	/	●
	数据共享域	●	/	/	/	/	●
	数据开放域	●	/	/	/	●	●
	数据运营域	●	/	/	●	●	●
政务大数据基础设施	基础资源平台	/	/	/	/	/	●
	基础安全平台	/	/	/	/	/	●
注：“●”代表存在参与关系，“/”代表不存在参与关系。							

4.4.2 政务大数据流转维度的参与方

根据政务大数据在数据流转过程中的角色类型，政务大数据参与方可分为数据提供者、数据接收者两类，各参与方的定义见表5，各参与方示例见附录A。

表5 政务大数据流转维度的参与方

角色	定义
数据提供者	向政务大数据域提供数据的组织、个人
数据接收者	从政务大数据域接收数据的组织、个人

一个组织或个人可以承担多个维度的多个参与方角色，同一维度的一个参与方角色也可以对应多个组织或个人。

5 政务大数据域安全要求

5.1 通用安全要求

政务大数据域应满足以下通用安全要求：

a）政务大数据域的参与方应按照GB/T 22239、GB/T 39786、GB/T 35273、GB/T 35274、GB/T 38664.2、GB/T 39477等要求对政务大数据进行保护；

b）政务大数据域的参与方应按照DB11/T 1918对政务大数据进行分级安全保护；

c）政务大数据域的参与方应按照GB/T 37988对自身数据安全保护能力进行评定；

d）平台运营者应按照GB/T 20269、GB/T 20271等要求对政务信息系统进行保护。

5.2 数据生产域

5.2.1 数据控制者安全要求

数据控制者应满足以下安全要求：

a）获得数据提供者的授权，并在授权范围内合法处理数据；

b）对数据生产者数据生产行为进行授权和监督管理；

c）制定数据生产规程，明确政务信息资源分类分级、目录编制、存储、备份、归档等相关要求；

d）具备对政务数据生产过程的安全审计能力，定期对数据生产者的数据生产行为进行审计；

e）制定安全策略并采取相应的安全措施，确保数据安全使用；

f）在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即采取应急处置措施。

5.2.2 数据生产者安全要求

数据生产者应满足以下安全要求：

a）遵守政务数据生产规程，在控制者授权范围内进行数据生产；

b）采用身份鉴别、加密、完整性校验、冗余等技术措施，确保数据的真实性、完整性、保密性和可用性；

c）在数据生产过程中，采取安全措施保障个人信息主体权益；

d）对生产数据进行分类分级并标识；

e）建立生产数据的数据资源目录，明确数据的使用范围和条件；

f）根据生产数据的重要性、量级、使用频率、敏感性等因素进行分域分级存储；

g）对生产数据进行定期备份，并适时进行归档；

h）记录数据生产过程。

5.2.3 数据提供者安全要求

数据提供者应满足以下安全要求：

a）保证所提供数据的合法性、真实性和有效性；

b）向数据控制者进行授权，明确所提供数据的使用范围和条件。

5.2.4 数据使用者安全要求

数据使用者应满足以下安全要求：

a）在授权范围内合法使用数据；

b）在数据使用过程中，采取相应的安全措施，避免重要数据和个人信息的泄露和滥用。

5.3 数据加工域

5.3.1 数据控制者安全要求

数据控制者应满足以下安全要求：

a）获得数据提供者的授权，并在授权范围内处理数据；

b）对数据加工者进行授权，明确授权目的和范围；

c）制定数据加工规程，明确政务信息资源分类分级、目录编制、清洗、脱敏、标识、存储、归档等相关要求；

d）设置严格的数据访问控制规则，采取限制数据加工终端外部接入的互联网地址等措施，保证数据加工在合法授权范围内，禁止未经授权的操作行为；

e）具备对政务数据加工过程的安全审计能力，对数据加工过程进行监督，并定期对数据加工者的数据加工行为进行审计；

f）在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据加工行为并采取相应的补救措施。

5.3.2 数据加工者安全要求

数据加工者应满足以下安全要求：

a）获得数据控制者的授权，并在授权范围内合法加工数据；

b）全面准确理解数据加工安全需求；

c）对数据进行分类分级，建立数据资源目录并进行数据标识；

d）根据业务需要采用泛化、抑制、干扰等技术，对敏感数据进行脱敏；

e）根据数据的重要性、量级、使用频率、敏感性等因素进行分域分级存储；

f）未经许可不得留存委托加工的数据；

g）对数据适时进行归档；

h）不得非法向他人转让委托加工的数据；

i）留存数据加工日志，并在数据加工报告中记录安全事件的处置情况。

5.4 数据共享域

数据控制者应满足以下安全要求：

a）获得数据提供者的授权，并在授权范围内合法共享数据；

b）对数据接收者进行授权，明确授权目的和范围；

c）建立数据共享目录，明确数据共享的范围和条件；

d）制定数据共享安全策略，采取权限控制、加解密、水印、脱敏、隐私计算、审计等安全技术措施，保证数据共享安全；

e）建立在数据共享完成后对数据共享通道缓存的数据进行安全删除的相关机制；

f）具备对政务数据共享过程安全审计能力，定期对数据共享行为进行审计；

g）在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据共享行为并采取相应的补救措施。

5.5 数据开放域

5.5.1 数据控制者安全要求

数据控制者应满足以下安全要求：

a）获得数据提供者的授权，并在授权范围内合法开放数据；

b）对数据使用者进行授权，明确授权目的和范围；

c）建立数据开放目录，明确数据开放的范围和条件；

d）制定数据开放安全策略，并对开放数据进行审核和安全检查，确保敏感数据、个人信息不向社会开放；

e）具备对政务数据开放过程的安全审计能力，定期对数据开放行为进行审计；

f）在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据开放行为并采取相应的补救措施。

5.5.2 数据使用者安全要求

数据使用者应满足以下安全要求：

a）在授权范围内合法使用数据；

b）保证开放数据使用环境和使用过程的安全性，以防数据的篡改和滥用。

5.6 数据运营域

5.6.1 数据控制者安全要求

数据控制者应满足以下安全要求：

a）获得数据提供者授权，并在合法范围内运营数据；

b）对数据运营者进行授权，明确授权的目的和范围；

c）建立数据运营规范，保证数据运营安全；

d）审核运营数据的应用场景，确保运营数据使用没有超出提供者的授权范围；

e）具备对政务数据运营过程的安全审计能力，定期对数据运营行为进行审计；

f）在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据运营行为并采取相应的补救措施。

5.6.2数据运营者安全要求

数据运营者应满足以下安全要求：

a）获得数据控制者的授权，并基于授权和数据运营规范合法运营数据；

b）对数据使用者进行授权，明确授权目的和范围，不得超出数据控制者的授权范围；

c）制定数据运营安全策略，采取技术和管理措施，保障运营数据安全；

d）支持基于区块链和数字水印技术实现对数据运营服务过程的溯源；

e）涉及数据交易活动的，提供证明数据交易合法性的授权文件；

f）不得非法向他人转让授权运营的数据。

5.6.3 数据使用者安全要求

数据使用者应满足以下安全要求：

a）在授权范围内合法使用数据；

b）保证数据使用环境和使用过程的安全性，以防数据的泄露和滥用；

c）涉及个人信息的，得到个人信息主体对数据使用者以及数据运营者、数据控制者等数据提供者的同意。

6 政务大数据域间协同安全要求

6.1 通用安全要求

政务大数据域间协同应满足以下通用安全要求：

a）数据提供者应确保数据来源的合法性；

b）数据提供者应对数据接收者进行授权，明确数据权责是否全部或部分转移给接收者；

c）数据接收者应采取必要的技术手段和管控手段，严格遵照数据提供者的授权开展数据处理，保护数据相关方合法权益；

d）数据接收者应确保数据安全保护级别不低于数据提供者，避免数据从高安全等级流向低安全等级；

e）数据提供者和数据接收者应采取数字签名等技术措施，保证数据提供者和数据接收者的真实性；

f）平台运营者应建立相应的安全控制措施，如冗余链路、数据传输加密等，保证数据传输过程中数据的安全性和完整性；

g）平台运营者应制定域间安全访问策略，并实施严格的访问控制。

6.2 数据生产域与数据加工域间协同安全

6.2.1 数据生产域安全要求

数据生产域应满足以下安全要求：

a）明确数据加工限制和约束条件，确保数据加工不能损害相关权利人的合法权益；

b）按照最小化原则提供用于加工的数据；

c）采取相应的措施，控制数据加工者对数据的访问。

6.2.2 数据加工域安全要求

数据加工域应满足以下安全要求：

a）接受加工委托时，提供其安全保障能力的证明材料；

b）验证接收数据的完整性及与数据加工需求的一致性；

c）将加工过程中发现异常数据及时告知对方，涉及敏感数据的在告知时应进行加密传输。

6.3 数据加工域与数据共享域间协同安全

6.3.1 数据加工域安全要求

数据加工域应满足以下安全要求：

a）接受加工委托时，提供其安全保障能力的证明材料；

b）验证接收数据的完整性及与数据加工需求的一致性；

c）将加工过程中发现异常数据及时告知对方，涉及敏感数据的在告知时应进行加密传输。

6.3.2 数据共享域安全要求

数据共享域应满足以下安全要求：

a）明确数据提供者的加工需求；

b）及时准确、完整的接收需要加工的数据，并提供给数据加工者；

c）及时将数据加工者发现的异常数据反馈给数据提供者。

6.4 数据生产域与数据共享域间协同安全

6.4.1 数据生产域安全要求

数据生产域应满足以下安全要求：

a）明确用于共享的数据的共享方式、范围、时效、授权条件及其他限制条件；

b）使用共享数据时，严格按共享规则使用，并对共享数据进行有效保护；

c）将使用过程中发现异常数据及时告知数据提供者，涉及敏感数据的在告知时应进行加密传输。

6.4.2 数据共享域安全要求

数据共享域应满足以下安全要求：

a）严格按照数据提供者的授权进行数据共享；

b）提供数据时，根据共享数据的安全等级确定无条件共享、有条件共享、不予共享等共享方式。

6.5 数据开放域与数据共享域间协同安全

6.5.1 数据开放域安全要求

数据开放域应及时发现禁止开放的敏感数据和个人信息，并告知数据提供者。

6.5.2 数据共享域安全要求

数据共享域应满足以下安全要求：

a）严格按照数据提供者的授权，遵照数据开放目录和开放计划，向数据开放域提供数据；

b）确保提供开放的数据不包含个人信息或敏感数据。

6.6 数据运营域与数据共享域间协同安全

6.6.1 数据运营域安全要求

数据运营域应满足以下安全要求：

a）提供其安全保障能力证明材料并获得数据运营授权；

b）未经提供者许可，不得留存共享获得的数据；

c）在数据运营过程中，及时发现不在授权范围内的重要数据和个人信息，并通知数据提供者；

d）定期向共享域报告数据安全运营情况，并提供相应的数据安全运营分析报告。

6.6.2 数据共享域安全要求

数据共享域应满足以下安全要求：

a）评估运营域数据运营环境与限制和约束条件，确保运营域的数据运营活动不损害相关权利人的合法权益；

b）审核运营域的数据运营场景和行为，确保数据运营服务没有超出授权范围；

c）提供运营数据时，保证数据运营者获得了授权并具备相应能力；

d）对数据运营过程进行安全监督、检查和定期审计，并督促数据运营域及时处置存在的运营安全问题。

6.7 数据共享域与数据共享域间协同安全

不同政务部门的数据共享域之间交换数据时应满足以下安全要求：

a）数据提供者应审核共享数据的应用场景和安全保护措施，确保共享数据没有超出提供者的授权范围；

b）数据提供者应建立敏感数据的脱敏安全策略，并按照安全要求进行脱敏；

c）数据接收者应按照共享数据提供者授权和安全要求对数据进行共享和保护；

d）数据接收者应建立检查机制，保障共享数据安全策略的正确配置与实施；

e）数据提供者和数据接收者应具备对政务数据交换过程的追溯和安全审计能力，定期对数据交换行为进行评估和审计，并及时处置存在的问题。

7 政务大数据基础设施安全要求

平台运营者应满足以下安全要求：

a）按照GB/T 22239、GB/T 39786、GB/T 35274、GB/T 35273等要求对政务大数据基础设施进行安全保护；

b）按照GB/T 37988的要求对自身数据安全保护能力进行评定；

c）通过技术和管理手段确保政务大数据基础设施安全；

d）具备提供统一身份认证、统一授权管理、数据密码保护、数据溯源、数据安全监测等安全服务的能力，以满足各政务大数据域的安全需求；

e）定期对政务大数据基础设施进行网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况；

f）实时监测政务大数据基础设施的安全状况，及时对信息安全隐患和事件进行发现和预警；

g）制定网络安全应急预案，定期开展应急演练，按照有关规定向相关机构报告网络安全事件，并及时进行应急处置。

附 录 A
（资料性）
域内资源、资产及参与方示例

A.1 政务大数据域的资源和资产示例

根据大数据应用场景的不同，各政务大数据域中所包含的资源和资产各不相同，表A.1给出了各域所包含的资源和资产示例。

表 A.1 政务大数据域的资源和资产示例

域类型	资源和资产
数据生产域	政务部门门户网站、政务信息系统等及相关数据
数据加工域	数据清洗、数据加工平台等及相关数据
数据共享域	共享交换平台、目录区块链系统等及相关数据
数据开放域	政务数据开放网站等及相关数据
数据运营域	金融专区、空间专区等数据专区及相关数据

A.2 政务大数据处理维度的参与方示例

表A.2给出了政务大数据处理维度的参与方的示例。

表 A.2 政务大数据处理维度的参与方示例

参与方	示例
数据生产者	政务部门、生产数据的企业等
数据控制者	政务部门等
数据加工者	信息技术服务外包机构等
数据运营者	金融专区、空间专区等数据专区运营企业等
数据使用者	个人、企业、政务部门等
平台运营者	政务部门、信息技术服务外包机构等

A.3 政务大数据流转维度的参与方示例

当政务大数据从政务部门A的数据生产域向数据加工域流动时，数据生产域提供数据，数据加工域接收数据，相应的，数据生产者就是数据提供者，数据加工者就是数据接收者，如图A.1所示。

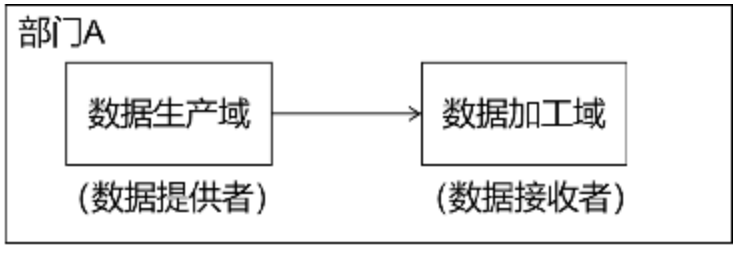

图 A.1 政务大数据在部门内部流转的参与方示例

当政务大数据通过数据共享域从政务部门A流向政务部门B时，政务部门A提供数据，政务部门B接收数据，相应的，政务部门A就是数据提供者，政务部门B就是数据接收者，如图A.2所示。

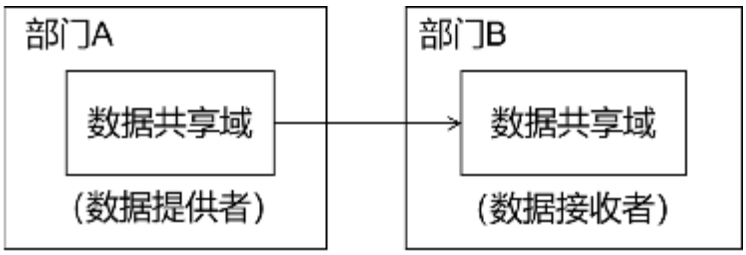

图 A.2 政务大数据跨部门流转的参与方示例

参 考 文 献

[1]促进大数据发展行动纲要（国发〔2015〕50号）
[2]政务信息资源共享管理暂行办法（国发〔2016〕51号）
[3]全国一体化政务大数据体系建设指南（国办函〔2022〕102号）
[4]北京市政务信息资源管理办法（试行）（京政发〔2017〕37号）
[5]北京市大数据行动计划工作方案（京政办发〔2018〕31号）