ICS 35.020
CCS L 70

DB3212

泰 州 市 地 方 标 准

DB3212/T 1118—2022

政务数据共享与开放安全管理规范

Government data opening and sharing management standard

2022-12-28 发布　　2022-12-28 实施

泰州市市场监督管理局　发布

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。

本文件由泰州市大数据管理局提出。

本文件由泰州市大数据管理局归口。

本文件起草单位：泰州市大数据管理局、泰州市标准化院。

本文件主要起草人：赵文涛、刘小芳、梁鑫晨、陈书剑、孙慧、王小冬、许鑫、施驰乐、吴薇、陈蓝生、李海鹏、张婧娴、王友成、郭健。

政务数据共享与开放安全管理规范

1 范围

本文件规定了政务数据共享与开放安全管理规范的总则、基本要求、组织管理、数据生命周期安全等要求。

本文件适用于泰州市政务数据的共享与开放。

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 25058 信息安全技术 网络安全等级保护实施指南.

GB/T 31722 信息技术 安全技术 信息安全风险管理

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 36073 数据管理能力成熟度评估模型

GB/T 36344—2018 信息技术 数据质量评价指标

GB/T 39295—2017 信息技术 大数据 术语

GM/T 0054 信息系统密码应用基本要求

3 术语和定义

GB/T 39295—2017 界定的以及下列术语和定义适用于本文件。

3.1

政务数据 government data

各级政务部门在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

注：根据可传播范围，政务数据一般包括可共享政务数据、可开放公共数据及不宜开放共享政务数据。

3.2

政务数据共享 government data sharing

各级政务部门因履行职责需要，使用其他政务部门的政务数据以及为其他政务部门提供政务数据的行为。

3.3

政务信息资源目录 government information resource catalog

通过对政务信息资源依据规范的元数据描述，按照一定的分类方法进行排序和编码的一组信息。

注：一般用以描述各个政务信息资源的特征，以便于对政务数据的检索、定位与获取。

3.4

政务数据开放 government data opening

政务部门在安全保密、公共利益导向前提下，面向公民、法人和其他组织以非排他形式提供政务数据的行为。

3.5

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。

4 总则

4.1　政务数据共享与开放安全管理采取主动防御、综合防范方针，坚持保障政务数据安全与促进应用发展相协调、管理与技术并重的原则，实行统一协调、分工负责、分级管理。政务数据管理相关方数据安全和信息化工作应同步规划、同步建设、同步运行。
4.2　政务数据共享与开放安全要求包括基本要求，组织管理、数据生命周期安全。各参与方应根据自身角色和责任遵照执行。
4.3　支撑政务数据共享的平台基础设施应符合附录 A 的要求。

5　基本要求

5.1　数据安全策略与规程

5.1.1　应制定满足业务需求的安全策略，明确安全方针、安全目标和安全原则。
5.1.2　应基于安全策略，建立相关的制度规程，形成以数据为核心的体系化数据安全制度体系。
5.1.3　应明确制度和规程分发机制，确保制度和规程分发至组织的相关部门、岗位和人员。
5.1.4　应建立策略、规程的评审和发布流程，明确适当的频率和时机对策略和规程进行更新，以确保其持续的适宜性和有效性。

5.2　数据供应链管理

5.2.1　应建立数据提供者、数据使用者、数据运营者安全管理规范，定义数据安全目标、原则和范围，明确数据提供者、数据使用者、数据运营者的安全责任和义务，并建立监督审核机制。
5.2.2　与数据提供者、数据使用者、数据运营者签署协议，明确数据的使用目的、供应方式、保密约定等。
5.2.3　应委托独立的运行监管方，对数据提供者、数据使用者和数据运营者的行为进行相关记录，利用技术工具对数据提供者、数据使用者和数据运营者的行为进行合规性审核与监督。
5.2.4　应建立完整的数据供应链和相关数据字典规则库，自动监测实际数据流动情况，实时分析数据流向与数据供应链遵循情况，发现异常并自动报警和阻断。

5.3　元数据管理

5.3.1　应建立数据服务元数据语义统一规范和管理规则，如口令策略、权限列表、授权策略。
5.3.2　应建立元数据访问控制策略，明确元数据管理角色及其授权控制机制，并通过技术手段实现对元数据管理角色的授权和访问管理。
5.3.3　应建立元数据操作审计制度，根据审计制度要求，采集元数据操作日志，确保元数据操作的可追溯。
5.3.4　应保证元数据的一致性和连续性，避免元数据错乱。
5.3.5　应建立统一的元数据管理平台，将各领域的元数据通过集中的平台进行提供。

5.4　运行监管

5.4.1　应制定数据生命周期各阶段数据访问和操作的日志记录规范要求和监管要求。
5.4.2　应根据日志记录规范和监管要求，对数据采集、传输、存储、处理、交换、销毁等过程进行有效的日志记录，实现政务数据共享全链路的可追溯。
5.4.3　应建立统一的数据访问和操作的日志记录和分析技术工具，该技术工具可对各类数据访问和操作的日志进行统一的处理和分析，实现对数据异常访问和操作的告警，实现对数据滥用、违规使用、缔约过失、越权使用等行为的识别、监控、预警和追责。
5.4.4　应对数据运营者实施的安全控制措施、变更管理、应急响应等进行持续监管，通过技术措施或文件审核等方式对数据运营者承诺的安全控制项进行评估验证。
5.4.5　应建立针对敏感数据的动态可持续的数据风险监管体系，周期性的对敏感数据的脆弱性、面临的安全威胁、安全措施的有效性等内容进行风险评估。

5.5　终端数据管理

5.5.1　应制订面向终端的数据安全管理规范，明确终端层面的数据防泄漏管理要求。

5.5.2 应建立并实施整体的终端安全解决方案，实现终端设备与组织机构内部员工的有效绑定，按照统一的部署标准在终端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、终端防泄漏等软件），对终端系统上的数据进行风险监控。

5.5.3 应采用身份鉴别、访问控制等手段对打印输出设备进行安全管控，并对用户账户在该终端设备上的数据操作进行日志记录。

5.6 数据防泄漏

5.6.1 应建立数据防泄露规范，明确需要进行数据泄露防护处理的应用场景和处理方法。

5.6.2 应支持基于终端使用、动态传输、静态存储的综合数据泄露防护机制。

5.6.3 应限制批量修改、拷贝、下载等操作的权限。

5.6.4 应提供数据防泄漏处理过程的日志记录，满足数据防泄漏处理安全审计要求。

6 组织管理

6.1 政务数据管理相关方

6.1.1 政务数据管理相关方包括：政务数据安全管理组织、政务数据提供者、政务数据使用者、政务数据运营者。

6.1.2 政务数据安全管理组织应履行政务数据安全管理、安全执行、安全审计、政务数据共享开放管理的职责：

a) 政务数据安全管理者负责数据安全相关领域和环节的决策，制定并审议数据安全相关制度，监督执行和组织落实业务部门数据安全相关工作；
b) 政务数据安全执行者负责数据安全相关领域和环节工作的执行，制定数据安全相关细则，落实各项安全措施，配合数据安全管理者开展各项工作；
c) 政务数据安全审计者对安全策略的适当性进行评价，帮助检测安全违规，并生成安全审计报告；
d) 政务数据共享开放管理者对数据共享交换等平台和过程进行管理，执行政务数据安全管理者分配的工作任务。

6.1.3 政务数据提供者是参与政务数据在开放、共享、交换、交易等过程的采集数据进行处理的人员或组织。

6.1.4 数政务据使用者在开放、共享、交换、交易等过程中获取政务数据的人员或组织。

6.1.5 政务数据运营者是依法依规对政务数据在开放、共享、交换、交易等过程中进行控制的人员或组织。

6.2 政务数据管理组织

6.2.1 政务数据安全管理者责任包括但不限于：

a) 确定数据的分类分级初始值，制定数据分类分级指南。与提供数据的业务部门合作，确定数据的安全级别；
b) 综合考虑法律法规、政策、标准、数据分析技术水平、组织所处行业特殊性等因素，评估数据安全风险，制定数据安全基本要求；
c) 对数据访问进行授权；
d) 建立相应的数据安全管理监督机制，监视数据安全管理机制的有效性；
e) 组织人员培训，应建立数据安全培训机制，定期组织开展数据安全专项培训。

6.2.2 政务数据安全执行者责任包含但不限于：

a) 根据政务数据安全管理者的要求实施安全措施；
b) 为政务数据安全管理者授权的相关方分配数据访问权限和机制；
c) 配合政务数据安全管理者处置安全事件；
d) 记录数据活动的相关日志；
e) 定期组织开展对数据开放、共享、交换、交易等过程的数据安全检查；定期对政务数据使用者的数据安全防护能力进行评估；
f) 当发生重大数据安全事件时，数据管理组织应牵头成立调查组对发生安全事件的相关方进行调查，调查组可以调阅、摘抄、复制与数据安全事件有关的资料，封存有关设备，进行调查取证；

根据调查结果对相关数据提供、管理、运营及使用的相关方进行责任追究，责令限期整改；对造成重大损失或者社会影响的，责令暂停相关业务，涉及违法犯罪的由公安机关依法查处。

6.2.3 政务数据安全审计者责任包含但不限于：

a) 审计数据活动的主体、操作及对象等相关属性，确保数据活动的过程和相关操作符合安全要求；
b) 定期审计数据安全的管理情况；
c) 出具数据安全审计报告；
d) 监督和推动各方对审计结果进行确认、整改、复测、关闭；
e) 对审计中的高危风险及时汇报给政务数据安全管理者，确保风险有人负责处置过程，并对处置过程进行验证。

6.2.4 政务数据共享管理者责任包含但不限于：

a) 建立数据资源共享管理制度，负责数据资源目录的编制、审核和维护；
b) 依据数据资源目录审核归集的数据资源，确保归集数据合规性、准确性和完整性；
c) 牵头制定数据分类分级标准，开展相关工作；
d) 牵头制定数据使用的策略和规则，对数据使用者的数据共享申请进行审批；
e) 对数据使用者的分析数据结果输出进行抽查。

6.3 政务数据提供者

政务数据提供者责任包括但不限于：

a) 向政务数据管理组织提供数据资源目录；
b) 遵循“一数一源”和必要及最小化的原则采集数据，不宜重复采集通过共享方式获取的数据资源；
c) 给出采集和提供数据的共享范围、共享期限、共享用途和数据保存期限；
d) 对政务数据使用者提交的数据共享申请，根据履职需要和最小化原则，进行审批授权；
e) 对共享的数据设置对应的数据分类分级标签；
f) 通过技术手段确保共享数据的完整性和一致性，并按照约定的频率更新数据。

6.4 政务数据使用者

政务数据使用者责任包括但不限于：

a) 基于业务场景向政务数据提供者或政务数据管理者申请数据共享，明确数据的使用目的、范围、期限、更新频率等具体使用需求；
b) 不再对脱敏后的个人信息和敏感数据进行再识别；
c) 根据共享数据的保存期限进行数据销毁工作；
d) 根据获取到的共享数据的安全级别，采取相应等级的安全防护措施进行防护；
e) 根据业务需求对共享数据进行再次加工时，联合政务数据管理者对加工后的数据进行识别和设置分类分级标签，并采取相应等级的防护措施进行安全防护；
f) 完整记录数据使用过程中的操作日志；
g) 明确数据使用的第一责任人。

6.5 政务数据运营者

政务数据运营者安全责任包括但不限于：

a) 进行书面安全承诺，承诺提供的产品和服务不包含恶意程序、隐蔽接口或未明示功能的模块等；
b) 建立并执行针对产品和服务安全缺陷、漏洞的应急响应机制和流程，在发现提供的产品和服务存在安全缺陷、漏洞时，立即采取修复或替代方案等补救措施，及时告知用户安全风险，并向数据管理者报告；
c) 收集用户信息应明确告知收集用户信息的目的、用途、范围和类型，在用户明示同意后，按照最少够用原则收集实现产品和服务功能所需的最少用户信息，并采取安全措施保护用户信息的安全；
d) 产品和服务上线前应告知政务数据管理者上线计划，并接受政务数据管理者或由政务数据管理者授权委托的服务方进行安全检查；

e) 建立内部监督审计机制，对提供服务的人员进行监督和审计，签订保密协议，确保其不泄露用户的业务数据；
f) 接受政务数据管理组织的安全监管工作，按监管要求提供相关交付件供政务数据管理者或监管服务方审核评估，并对通报的安全风险进行及时整改；
g) 根据政务数据管理者制定的安全策略和规则进行数据的访问授权管理工作；
h) 提供服务 API 的用户鉴别、鉴权和访问控制的能力，并支持服务 API 的调用日志记录和外发；采取措施保障服务 API 自身的安全性，确保服务 API 具备防重放、代码注入、拒绝服务攻击等攻击防护能力；提供服务 API 过载保护的能力，实现不同服务等级用户间业务的公平性和系统整体性处理能力的最大化；
i) 对归集的数据保留原始表，不做任何加工清洗，以满足溯源、数据质量核查等需求；
j) 提供数据 ETL 服务的应根据质量规则进行标准化处理，并通过技术手段保障数据的一致性，对所有的 ETL 过程应记录日志，并可提供给第三方进行审计；
k) 提供数据同步服务的通过技术手段保障数据同步过程的一致性，记录数据同步过程的所有日志，并可提供给第三方进行审计；
l) 提供数据分析计算服务的应配合政务数据管理者或政务数据使用者对新生成的数据进行识别和设置分类分级标签。

7 数据生命周期安全

7.1 数据归集

7.1.1 数据分类分级

7.1.1.1 数据分类分级应符合 DB3212/T XXXX—2022 的要求。
7.1.1.2 应针对具体业务场景，结合数据敏感度等级，确定场景数据使用风险等级。
7.1.1.3 应根据数据敏感程度等级、数据影响程度等级确定相应的保护措施。安全保护等级分级见附录 B 的要求。
7.1.1.4 安全保护措施的选择应依据定级结果，安全保护措施应符合 GB/T 22239 以及附录 C 的要求。
7.1.1.5 应建立数据分级分类制度性文件管理措施，包括岗位职责、统一管理、定期更新、变更审核等。
7.1.1.6 应建立人工打标与基于数据内容规则自动识别打标相结合的机制。

7.1.2 数据采集

7.1.2.1 采集的数据应确保来源真实有效、合法正当，同时应明确数据共享范围和用途。
7.1.2.2 采集的数据应保留原始表，不做任何加工清洗，以满足溯源、数据质量核查等需求。

7.1.3 数据源鉴别及记录

7.1.3.1 应采取技术手段对归集数据的数据源进行识别和记录，记录信息包含业务处理人员、处理系统、IP 地址、处理时间、处理方式等，并进行有效存储，确保事件追溯时的信息可用性，能追踪原始数据来源。
7.1.3.2 应采取技术手段对分发的数据进行溯源，如明文水印、密文水印等。
7.1.3.3 应对关键的溯源信息进行备份和安全保护。
7.1.3.4 应采取访问控制、加密等技术措施保证溯源信息的完整性和保密性。
7.1.3.5 应支持溯源信息的存储，存储时间至少 12 个月。

7.1.4 数据质量

7.1.4.1 数据提供方提供的数据质量应符合 GB/T 36344—2018 中规定的数据数量指标的要求。
7.1.4.2 数据提供方有信息系统支撑的数据应提供结构化文件，并在汇聚数据时同步提供数据字典和码表，确保数据的可读可理解。
7.1.4.3 通过接口方式对接的，数据提供方要遵循接口传输规范，具有完整的日志记录，保证数据可用。

7.1.4.4　数据管理方归集的政务数据应确保数据可读、可理解、可用。
7.1.4.5　数据管理方所归集的数据要保持独立可用，避免多类业务数据混合提供。
7.1.4.6　数据管理方应利用技术工具对关键数据进行质量管理和监控，实现数据质量异常告警。

7.2　数据传输

7.2.1　应明确需要进行传输加密的业务场景，支持对个人信息和重要数据的加密传输，采用的密码技术应符合 GM/T 0054 的规定。
7.2.2　应提供对传输通道两端进行主体身份鉴别和认证的技术方案和工具。
7.2.3　应提供对传输数据的完整性进行检测并执行恢复控制的技术方案和工具。
7.2.4　应提供对数据传输安全策略的变更进行审核和监控的技术方案和工具，对通道安全策略配置、密码算法配置、密钥管理等保护措施进行审核及监控。

7.3　数据存储与访问

7.3.1　数据存储

7.3.1.1　应建立各类数据存储系统的安全配置规则，采取技术手段和工具支撑数据存储系统的安全管理。
7.3.1.2　应提供工具支撑存储介质及逻辑存储空间的安全管理，如权限管理、身份鉴别、访问控制等，防止存储介质和逻辑存储空间的不当使用。
7.3.1.3　应具备多租户数据存储安全隔离能力。
7.3.1.4　应定期检查数据存储系统安全配置以符合基线的一致性要求。
7.3.1.5　应定期探查存储系统的数据是否符合相关合规性的要求。
7.3.1.6　应采用碎片化分布式离散存储技术保存数据资源，并具有完整性验证机制。
7.3.1.7　应支持采用符合国家认定的密码算法对高敏感数据进行加密存储，平台服务商不得掌握密钥。

7.3.2　数据备份与恢复

7.3.2.1　应建立数据存储冗余策略、管理制度与规程，明确定义数据复制、备份和恢复的范围、频率、工具、过程、日志记录规范、数据保存时长等。
7.3.2.2　应建立用于数据备份、恢复的统一技术工具，并将具体的备份的策略固化到工具中，保证相关工作的自动化执行。
7.3.2.3　应建立数据复制、数据备份与恢复的定期检查和更新工作程序，包括数据副本更新频率、保存期限等，确保数据副本或备份数据的有效性。
7.3.2.4　过期存储数据及其备份数据应采用彻底删除或匿名化的方法进行处理。

7.3.3　数据访问控制

7.3.3.1　应建立数据资源安全访问策略，由授权主体进行访问策略配置，授予数据使用者为完成各自任务所需要的最小权限。访问控制的范围应包括与数据资源访问相关的主体、客体以及它们之间的操作。
7.3.3.2　应采用基于用户组或角色的方法，保障数据使用者访问数据资源时权限明确。
7.3.3.3　应建立用户口令长度、口令生存周期、口令复杂度等管理策略，保证基于口令的身份鉴别安全性。
7.3.3.4　关键系统应采用口令、密码技术、生物技术等 2 种及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应使用国密密码技术来实现。
7.3.3.5　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。
7.3.3.6　应采用必要的措施使数据使用者的访问和修改等行为具有不可抵赖性。

7.4　数据处理

7.4.1　数据脱敏

7.4.1.1　应建立数据脱敏规范，明确需要脱敏处理的应用场景和处理方法。

7.4.1.2 需保持数据集业务属性的场景，应采用重排、均化、排序映射、规整、偏移取值、截断、掩码屏蔽等方式脱敏。
7.4.1.3 需保持数据业务属性的场景，应采用加密、替换、固定偏移、局部混淆、乱序、随机化、变换等方式脱敏。
7.4.1.4 敏感度较高的数据，应采用加密、有损、散列、删除等方式脱敏。
7.4.1.5 应提供数据脱敏处理过程日志记录，满足数据脱敏处理安全审计要求。

7.4.2 数据使用

7.4.2.1 应制定整体的数据权限管理制度，规定了各参与方身份及访问权限的授予、变更、撤销等流程，以及数据全生命周期的管理要求和责任制。
7.4.2.2 应定义并执行了统一的身份及访问管理流程，各系统均遵循规范的身份及访问管理流程对用户访问数据资源进行管理，并定期审核当前的数据资源访问权限是否符合身份及访问管理的规范要求，身份及访问管理应遵循最少够用和职责分离的原则。
7.4.2.3 应建立数据使用正当性的监督审核机制，保证在数据使用声明的目的和范围内对受保护的个人信息、重要数据等数据进行使用和分析处理。
7.4.2.4 应建立统一的身份认证平台，对各系统的用户和数据资源进行权限管理，遵循做小够用的原则，并依据数据使用目的建立相应强度或粒度的访问控制机制。

7.4.3 数据处理环境

7.4.3.1 数据处理系统或平台应与身份认证平台实现联动，用户在使用数据处理系统或平台前已获得了授权
7.4.3.2 应保证对不同数据使用者在数据处理平台中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制。
7.4.3.3 应建立数据处理日志管理工具，记录用户在数据处理平台上的加工操作，以备后期追溯。
7.4.3.4 应对用户在数据处理平台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。

7.5 数据共享开放安全

7.5.1 数据导入导出

任何数据都不应导入导出。

7.5.2 数据开放

7.5.2.1 政务数据开放应实行分级管理，按照开放属性分为无条件开放和依申请开放，依申请开放类数据应明确管理流程，需记录申请、审批和签发管理的过程。
7.5.2.2 政务数据开放前，应对拟开放的数据进行脱敏、匿名化、去标识化处理，防止泄露商业秘密、个人隐私。
7.5.2.3 依申请开放类数据，宜将数据服务封装成接口，供审批通过的数据申请方调用，应记录调用事件和事件日志并监控流量，定期开展安全审计。
7.5.2.4 数据开放接口应采用防重放、防篡改等技术，保障数据的保密性和完整性。

7.5.3 数据共享

7.5.3.1 应建立数据获取和使用安全规范，明确数据使用者的数据获取方式、服务接口、授权机制和数据使用的权限范围等。
7.5.3.2 应建立规范的数据共享审核流程，确保没有超出数据提供者所允许的数据授权使用范围。
7.5.3.3 数据使用者应采用数据服务接口方式获取共享数据资源。
7.5.3.4 应建立数据服务接口调用的安全规范，包括接口名称、接口参数、接口安全要求等。
7.5.3.5 应制定数据服务接口安全控制策略，提供对数据服务接口的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等，并对数据服务接口调用的参数进行限制或过滤，一旦发现异常会触发告警机制。

7.5.3.6　应统一收集数据服务接口调用的相关记录日志，并建立相应针对数据接口调用的审计工具，对数据接口调用情况进行定期审计。

7.6　数据销毁

7.6.1　数据销毁处置

7.6.1.1　应制定数据销毁规范，提出各类数据销毁场景应采用的销毁手段，明确销毁方式和销毁要求。
7.6.1.2　应建立数据销毁的审批和记录流程，并设置数据销毁监督角色，监督数据销毁操作过程。

7.6.2　存储媒体销毁

7.6.2.1 应依据存储媒体存储内容的重要性，明确不同类型存储媒体的销毁方法。
7.6.2.2 应对存储媒体销毁的登记、审批、交接等过程进行监控。
7.6.2.3 存储媒体如不需继续使用，应采取不可恢复的方式对存储媒体进行销毁，包括但不限于消磁销毁、焚烧、粉碎等。
7.6.2.4 存储媒体如需继续使用，应通过多次复写等方式安全的擦除数据，保证数据擦除所填充的字符完全覆盖存储数据区域。

附 录 A
（规范性）
政务数据共享的平台基础设施

A.1 政务数据开放共享系统参考架构

政务数据开放共享系统参考架构由网络设施、数据资源、平台设施、安全保障和管理评价五部分组成，图 A.1 描述的参考架构适用于泰州市数据共享交换系统的建设，同时满足各级系统逐级对接要求。其中：

a) 网络设施：为政务数据开放共享提供统一、通达的网络基础设施支撑；
b) 数据资源：为政务数据开放共享提供数据资源，包括政务信息资源目录和政务数据内容；
c) 平台设施：基于政务数据的开放目录和共享目录提供开放和共享服务的平台设施，支撑政务数据使用者可通过平台从政务数据提供者获取数据；
d) 安全保障：提供政务数据采集、传输、处理、存储、使用等环节的安全保护；
e) 管理评价：提供整个开放共享的服务流程管理和考核评价。
f) 标准规范：为政务数据开放共享提供统一的标准、接口、流程。

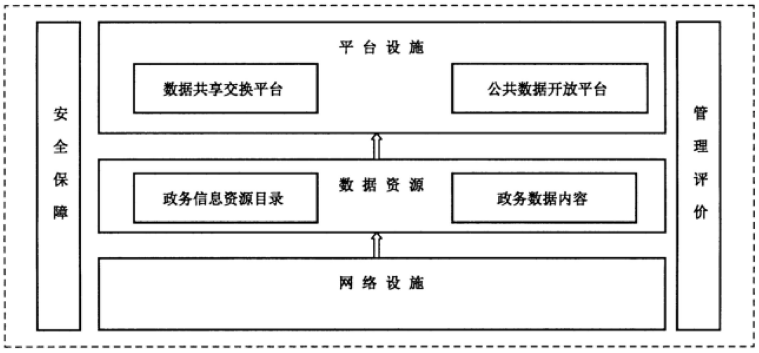

图 A.1 政务数据开放共享系统参考架构

A.2 网络设施要求

网络设施的基本要求如下：

a) 政务数据共享交换应通过统一的电子政务内网和电子政务外网开展；非涉密系统在电子政务外网，涉密系统在电子政务内网；共享平台（内网）应按照涉密信息系统分级保护要求，依托国家电子政务内网建设和管理；共享平台（外网）应按照国家网络安全相关制度和要求，依托国家电子政务外网建设和管理。
b) 政务数据共享交换系统应基于电子政务外网建设政务信息共享网站。
c) 公共数据开放应通过互联网开展。
d) 公共数据开放应基于互联网建设公共数据开放服务门户，基于统一的电子政务外网建立公共数据管理平台。

A.3 数据资源要求

A.3.1 政务信息资源目录要求

政务信息资源目录要求如下：

a) 政务信息资源目录是开展各政务部门之间数据共享交换及向社会开放公共数据的依据和导引。
b) 政务信息资源目录编制工作应包括政务信息资源分类、元数据描述、代码规划和目录编制，以及相关工作的组织、流程、要求等方面的内容。

c) 开放目录和共享目录独立存在时，同一政务信息资源的相同信息项信息在共享和开放目录中应统一。

d) 政务信息资源目录中的政务信息资源应按照资源属性、涉密属性、共享属性、层级属性等属性进行分类：

1) 政务信息资源目录按资源属性应分为基础信息资源目录、主题信息资源目录、部门信息资源目录等类型；

2) 政务信息资源目录按涉密属性应分为涉密政务信息资源目录和非涉密政务信息资源目录；

3) 政务信息资源目录按共享属性应分为无条件共享、有条件共享、不予共享三种类型；

4) 政务信息资源目录按层级属性应分为部门政务信息资源目录、国家政务信息资源目录。

f) 政务信息资源目录元数据应包括核心元数据和扩展元数据。

g) 政务信息资源目录核心元数据应包括信息资源分类、信息资源名称、信息资源代码、信息资源提供方、信息资源提供方代码、信息资源摘要、信息资源格式、信息项信息、共享属性、开放属性、更新周期、发布日期、关联资源代码。

A.3.2 政务数据内容要求

A.3.2.1 数据格式要求

数据格式要求如下：

a) 政务数据提供者应提供可机读的电子格式及相关软件版本信息；

b) 数据集应以开放的、非专属的格式提供，包括电子文件格式、电子表格格式、图形图像文件格式、流媒体文件格式、自描述格式等，

c) 数据库类格式需明确具体的数据库表结构定义；

d) 特殊行业领域数据应由数据提供方提出其特殊行业领域的通用格式；

e) 无法按照要求的形式提供数据的，可通过安排查阅相关资料、提供复制件或者其他适当形式提供。

A.3.2.2 数据质量要求

A.3.2.2.1 数据质量责任要求

数据质量责任要求如下：

a) 政务数据提供者应对提供的数据质量负责；

b) 原始数据提供者应对原始数据质量负责；

c) 数据加工者应对加工后的数据质量负责。

A.3.2.2.2 数据质量要求

通过政务数据共享交换平台和开放平台提供的数据质量要求如下：

a) 规范性：数据信息项定义应优先采用国家、行业相关数据标准，实施开放共享数据工程前应先统一数据标准；

b) 完整性：对于应满足需求的数据记录不应有缺失、重复，数据信息应完整，对敏感数据脱敏应保证最小颗粒度数据的完整展现；

c) 一致性：不同数据集中描述同一对象的同一度量值在信息含义上不可冲突；

d) 准确性：数据记录的内容应真实反映实际情况且有效，不能存在异常或错误，不能出现不可识别的内容；

e) 数据质量需求、数据质量检查、数据质量分析、数据质量提升等数据能力要求应遵循 GB/T 36073 的规定。

A.3.2.2.3 数据更新与完善要求

政务数据更新与完善要求如下：

a) 应根据情况变化对政务信息资源目录进行更新维护；

b) 应建立政务信息资源更新机制，进行动态管理；

c) 政务数据提供者应确保提供的数据信息完善，确保数据得到及时、持续更新；

d) 开放共享的信息内容发生变化时，政务数据提供者应当及时报告本级政务信息资源主管部门，更新相应政务信息资源目录和内容，并通知该政务数据使用者；
e) 政务数据使用者应当及时比对和更新所获取的政务信息资源，确保数据一致性。

A.4 平台设施要求

A.4.1 政务数据共享交换平台要求

政务数据共享交换平台要求如下：
a) 各级政务数据共享交换平台的建设要实现上下联动、纵横协管，保证政务数据的统一汇聚、资源整合和集中开放；
b) 应对已存在的多个共享交换系统进行整合，完成整合后的接入统一的数据共享交换平台，形成统一平台，实现政务信息资源跨部门共享；
c) 共享交换平台应包括目录系统、对接系统，交换系统、发布系统、数据资源管理系统、共享门户、运行监控系统等，
d) 共享交换平台应具备监控和管理系统，对平台进行监控管理、异常分析、考核等，实现对信息资源共享交换平台中的基础设施和业务系统集中监控和管理；
e) 共享交换平台应具备安全保障机制，按照信息系统安全等级保护要求构建数据存储环境、应用系统环境、运行管理机制，确保政务数据安全和公民个人数据合法应用，保证数据、网络和接入等多方面的安全要求。

A.4.2 公共数据开放平台要求

公共数据开放平台要求如下：
a) 开放平台应包括数据开放服务网站和数据管理平台；
b) 开放平台应实现数据开放服务、数据开放管理、安全脱敏、流向追踪等功能；
c) 开放平台应提供搜索、分类导航、数据内容预览及与使用者的交互等功能，其中，交互功能应包 括数据集评价功能、数据请求功能等；
d) 开放平台应提供明确充分的数据开放许可授权协议，保障用户免费获取、不受歧视、自由利用和分享数据的权利，授权条款可包含在开放平台的免责条款或用户协议中。

A.5 安全保障要求

政务数据安全保障的基本要求如下：
a) 应针对所要开放共享的数据进行风险分析和管理，应遵循 GB/T 31722 的规定；
b) 应根据风险分析结果确定所要开放共享的数据所涉及的安全保障等级，应遵循 GB/T 22239、GB/T 25058 的规定；
c) 对于个人信息类数据，宜遵循 GB/T 352737 的规定；
d) 应基于风险分析结果和所确定的安全保障等级以及个人信息保护要求，制定信息安全策略并实施动态管理；
e) 应按照信息安全策略建立、运行和维护相应的信息安全体系；
f) 宜适时进行安全评估并在必要时对已经建立的信息安全体系做相应调整，宜遵循 GB/T 18336 的规定。

A.6 管理评价要求

管理评价要求如下：
a) 应由政务数据使用者根据需要提出开放共享服务需求；
b) 政务数据提供者应及时响应开放共享服务需求；
c) 应建立政务数据共享工作评价机制；
d) 应建立数据开放程度评价的评价原则、评价指标体系和评价方法。

A.7 标准规范要求

标准规范要求如下：
a) 应由政务数据管理者统筹制定标准规范；

b） 政务数据标准规范应与国家、行业标准以及相关法律法规相衔接；
c） 应建立政务数据标准规范使用评价机制；
d） 应根据政务数据标准规范使用评价及时制修订相关标准规范。

附 录 B
（规范性）
安全保护等级

B.1 不同级别的政务数据，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的数据等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。政务数据定级后，可能形成的定级结果见表B.1。

表 B.1 安全保护等级

判定等级	判定标识	判定标准
L4	涉密数据	涉及国家安全、国民经济、民生大事、军事机密等方面的数据；数据被破坏后，会对社会秩序和公共利益造成严重损害，或对国家安全造成损害。
L3	敏感数据	涉及个人或组织人身财产安全、公共利益、社会秩序等方面的数据；数据被破坏后，对公民、法人和其他组织的合法权益造成严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全。
L2	受限数据	涉及个人或组织的基本信息、基本活动信息，可小范围内公开或有条件开放共享的数据；数据被破坏后，对公民、法人和其他组织的合法权益造成一般损害，但不损害国家安全、社会秩序和公共利益。
L1	公开数据	依法公开披露的数据；数据被破坏后，对社会秩序、公共利益以及对公民、法人和其它组织的合法权益均无影响。

附 录 C
（规范性）
安全保护措施

C.1 安全保护等级措施

依据安全保护等级采取各种安全措施时，还应考虑以下总体性要求，保证等级保护对象的整体安全保护能力：

a) 构建纵深的防御体系，在采取由点到面的各种安全措施时，在整体上还应保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证等级保护对象整体的安全保护能力。应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次落实本标准中提到的各种安全措施，形成纵深防御体系。

b) 采取互补的安全措施，在将各种安全控制落实到特定等级保护对象中时，应考虑各个安全控制之间的互补性，关注各个安全控制在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，保证各个安全控制共同综合作用于等级保护对象上，使得等级保护对象的整体安全保护能力得以保证。

c) 保证一致的安全强度，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到等级保护对象的各个层面，在实现各个层面安全功能时，应保证各个层面安全功能实现强度的一致性。

d) 应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上削弱。例如，要实现双因子身份鉴别，则应在各个层面的身份鉴别上均实现双因子身份鉴别；要实现基于标记的访问控制，则应保证在各个层面均实现基于标记的访问控制，并保证标记数据在整个等级保护对象内部流动时标记的唯一性等。

e) 建立统一的支撑平台，使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术或可信技术，为了保证等级保护对象的整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。

f) 进行集中的安全管理，实现集中的安全管理、安全监控和安全审计等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制在可控情况下发挥各自的作用，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

C.2 第一级可参考安全控制措施

C.2.1 安全通信网络

应保证政务大数据平台不承载高于其安全保护等级的大数据应用。

C.2.2 安全计算环境

大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。

C.2.3 安全建设管理

大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。

C.3 第二级可参考安全控制措施

C.3.1 安全通信网络

应保证大数据平台不承载高于其安全保护等级的大数据应用。安全计算环境本方面控制措施包括：

a) 大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别；
c) 大数据平台应为大数据航用提供管控其计算和存储资源使用状况的能力；
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
g) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理。

C.3.2 安全建设管理

本方面控制措施包括：
a) 大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

C.3.3 安全运维管理

应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。

C.4 第三级可参考安全控制措施

C.4.1 安全通信网络

本方面控制措施包括：
a) 应保证大数据平台不承载高于其安全保护等级的大数据应用；
b) 应保证大数据平台的管理流量与系统业务流量分离。

C.4.2 安全计算环境

本方面控制措施包括：
a) 大数据平台应对数据采集终端，数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
b) 大数据平台应能对不同客户的大数据应用实施标识和整别；
c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力；
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
e) 大数据平台应屏蔽计算，内存、存储资源故障，保障业务正常运行；
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
g) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；
h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
e) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
f) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
g) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
h) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
i) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；

j) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。

C.4.3 安全建设管理

本方面控制措施包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容
c) 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够成相当的安全防护能力。

C.4.4 安全运维管理

本方面控制措施包括：

a) 应建立数字贷产安全管理策略，对数据全生命周期的操作规范、保护措施，管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
b) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏成去标识的使用场景和业务处理流程；
c) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

C.5 第四级可参考安全控制措施

C.5.1 安全通信网络

本方面控制措施包括：

a) 应保证大数据平台不承载高于其安全保护等级的大数据应用；
b) 应保证大数据平台的管理流量与系统业务流量分离。

C.5.2 安全计算环境

本方面控制措施包括：

a) 大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别；
c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力；
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
g) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；
k) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
l) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
m) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
n) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
o) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；

p） 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；
q） 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；
r） 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

C.5.3 安全建设管理

本方面控制措施包括：
a） 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b） 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容：
c） 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

C.5.4 安全运维管理

本方面控制措施包括：
a） 应建立数字资产安全管理策略，对数据全生命周期的操作规范，保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
b） 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
c） 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
d） 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。
e） 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
f） 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
g） 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
h） 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
i） 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
j） 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；
k） 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；
l） 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

C.5.5 安全建设管理

本方面控制措施包括：
a） 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b） 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；
c） 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

C.5.6 安全运维管理

本方面控制措施包括：

a) 应建立数字资产安全管理策略，对数据全生命周期的操作规范，保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
b) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程
c) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。