ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

数据安全技术 政务数据处理安全要求

Data security technology—Security requirements for government data processing

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本稿完成时间：2024 年 4 月 8 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：国家信息中心、中国电子技术标准化研究院、贵州省信息中心、北京市大数据中心、深信服科技股份有限公司、中国科学院信息工程研究所、江西省信息中心、安徽省信息中心、广东省政务服务数据管理局、浙江省大数据发展管理局、无锡大数据管理局、浙江省发展测评有限公司等。

本文件主要起草人：徐春学、任飞、罗海宁、焦迪、宋博韬、于晶、罗华洋、赵莹、王君、程路遥、朱典、程子栋、田之洋、王鹏彪、徐羽佳等。

数据安全技术 政务数据处理安全要求

1 范围

本文件规定了政务数据处理的安全要求，明确了政务数据处理安全管理要求、政务数据处理安全技术要求、政务数据处理中的个人信息保护要求、政务数据处理安全运营要求和政务数据处理安全监督要求。

本文件适用于指导政务部门及其技术支撑单位规范政务数据处理活动，也可为监管部门、第三方机构进行监督管理和评估提供参考。

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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 38664.1—2020 信息技术 大数据 政务数据开发共享 第1部分：总则

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786—2021 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—2022、GB/T 38664.1—2020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

各级政务部门及其技术支撑单位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。

[来源：GB/T 38664.1—2020，定义 3.1，有修改]

3.2

政务数据处理 government data processing

政务数据的收集、存储、使用、加工、传输、提供、公开、销毁等活动。

3.3

政务数据处理者 government data processor

对政务数据进行收集、存储、使用、加工、传输、提供、公开、销毁等活动的个人或组织。

4 缩略语

下列缩略语适用于本文件。

SFTP：安全文件传输协议（Secured File Transfer Protocol）

5 政务数据处理安全要求框架

政务数据处理安全要求框架由五个部分组成，如图1所示，包括政务数据处理安全管理要求、政务数据处理安全技术要求、政务数据处理中的个人信息保护要求、政务数据处理安全运营要求和政务数据处理安全监督要求。

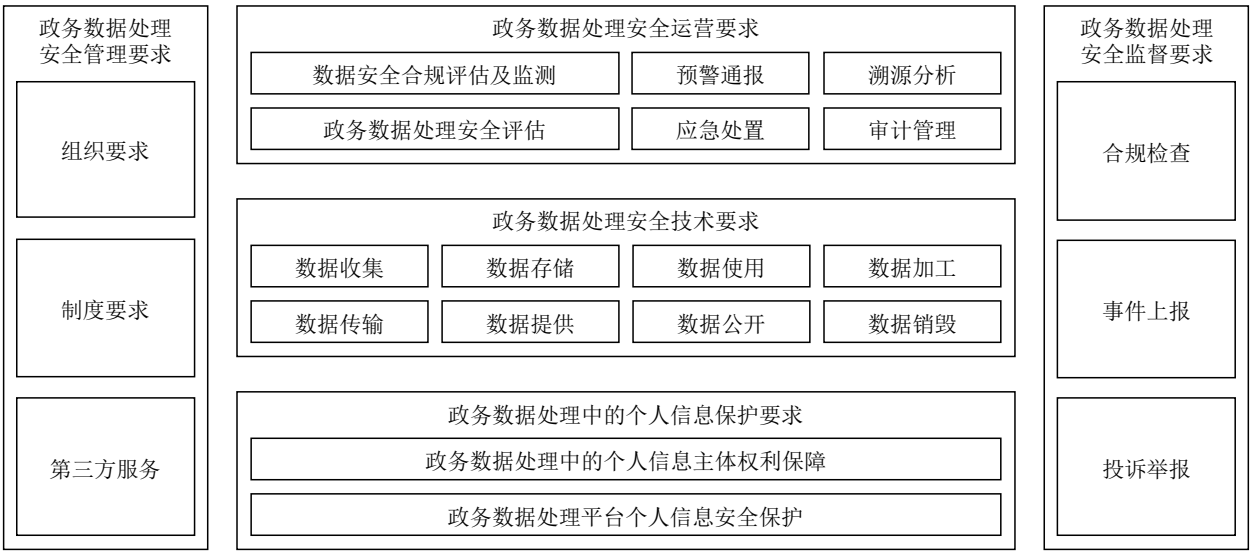

图1 政务数据处理安全要求框架

在政务数据处理安全管理方面，从组织、制度和第三方服务等三个方面提出安全管理要求。在政务数据处理安全技术方面，针对数据收集、存储、使用、加工、传输、提供、公开、销毁等政务数据处理活动提出安全技术要求。在政务数据中的个人信息保护方面，从个人信息主体权利保障和个人信息安全保护方面提出相应的安全要求。在政务数据处理安全运营方面，提出数据安全合规评估与监测、政务数据处理安全评估、预警通报、应急处置、溯源分析和审计管理等安全要求。在政务数据处理安全监督方面，明确了合规检查、事件上报及投诉举报等安全要求。

6 政务数据处理安全管理要求

6.1 政务数据处理安全组织要求

6.1.1 概述

政务数据处理活动的组织应包含决策层、管理层、执行层和监督层。决策层主要职责是对政务数据处理安全制定指导方针和政策，并提供安全保障资源；管理层主要职责是落实决策层所制定的相关政策，制定政务数据处理管理规范和制度，并组织推进数据安全管理工作；执行层主要职责是执行决策层和管理层所制定的政策、规范和制度，保障政务数据处理安全；监督层主要职责是依据决策层和管理层所制定的相关政策、规范和制度，监督执行层针对政务数据处理相关政策、规范和制度的落实情况，对于未能落实相关制度和规范的政务数据处理者采取安全管理措施。

6.1.2 决策层

决策层由政务数据处理者所在单位数据安全领导小组的成员组成，具体职责应包括：

a) 制定政务数据处理的整体安全目标和安全发展规划；

b） 发布政务数据处理的安全管理制度及规范；
c） 为政务数据处理的安全规划、设计、建设、实施、运营等全过程提供资源保障；
d） 为政务数据处理中发生的重大数据安全事件实施协调与决策；
e） 与国家或地方数据安全相关监督管理部门进行沟通协调。

6.1.3 管理层

管理层由政务数据处理者所在业务部门的管理人员及专职的数据安全管理部门人员组成，具体职责应包括：

a） 制定业务部门数据安全管理制度及规范，明确政务数据处理相关权责
b） 制定业务部门数据安全方案并组织实施；
c） 协调、落实政务数据安全决策层的决策；
d） 组织业务部门的政务数据安全业务与技术培训；
e） 牵头网络安全等级保护、信息系统密码应用安全等工作的开展。

6.1.4 执行层

执行层由政务数据处理者组成，具体职责应包括：

a） 实施政务数据安全方案；
b） 执行政务数据安全制度及规范；
c） 政务数据安全运维及运营；
d） 管理政务数据资源；
e） 政务数据安全风险监测；
f） 政务数据安全风险评估；
g） 政务数据安全漏洞监测及修复；
h） 政务数据安全事件处置及溯源分析。

6.1.5 监督层

监督层由政务数据处理者所在单位的安全监督和审计人员组成，具体职责应包括：

a） 对政务数据处理的数据安全制度与规范执行情况进行监督；
b） 对政务数据处理过程中的安全事件处置过程与结果进行监督；
c） 对政务数据处理过程中的安全风险管理措施进行监督和审计；
d） 将政务数据处理过程中的安全监督结果及时报告给决策层；
e） 对网络安全等级保护、信息系统密码应用安全等工作的执行情况进行监督。

6.2 政务数据处理安全制度要求

本项要求包括：

a） 应建立政务数据处理的组织保障机制；
b） 应制定政务数据处理的安全管理制度；
c） 应明确政务数据处理的数据安全负责人，处理个人信息达到国家网信部门规定数量应当指定个人信息保护负责人，将负责人的姓名、联系方式等报送给相关主管部门；
d） 应制定政务数据分类分级规范，明确政务数据的类别和级别，并识别个人信息、重要数据；
e） 应制定针对政务数据处理的数据安全管理规范，明确基于数据分类分级的安全管理措施，以及数据访问授权及审批机制等；
f） 应制定政务数据处理的个人信息安全管理规范，明确个人信息、敏感个人信息的安全管理措施；

g） 应制定政务数据处理的安全运维规范，明确数据安全风险监测、数据安全应急处置、数据安全风险评估、数据安全审计、数据备份恢复等相应措施要求；
h） 应定期审核和更新相关的政务数据安全管理规范，包括政务数据分类分级规范政务数据处理的个人信息安全管理规范和政务数据处理的安全运维规范等；
i） 应组织开展政务数据处理安全教育培训，每年组织开展全员数据安全教育培训，并依据培训反馈效果定期对教育培训计划进行审核和更新；
j） 应制定政务数据处理的安全报告制度，明确数据安全事件报告及数据安全风险评估报告等制度要求；
k） 对于处理政务数据的信息系统，应按照网络安全等级保护基本要求开展防护，并遵循 GB/T 22239-2019 对应级别要求；
l） 对于处理政务数据的信息系统，应制定密码应用安全管理制度，并遵循 GB/T 39786-2021 对应级别要求。

6.3 政务数据处理第三方服务安全要求

本项要求包括：
a） 委托他人建设、维护政务数据处理设施并处理政务数据，委托方应经过严格审批程序选择受托方，并监督受托方履行政务数据处理相关的安全要求；
b） 受托方留存、使用或者向他人提供政务数据，应依据法律、法规的规定和合同约定，未经授权不应访问、修改、披露、利用、转让、销毁政务数据资源；
c） 受托方应建立数据处理组织保障数据处理的安全，委托方承担组织保障监督层的相关职责；
d） 受托方应建立人员安全管理制度，明确招聘、录用、培训、考核、选拔、上岗、调岗、离岗等环节中人员安全管理的操作规程，对参与政务数据处理的人员开展必要的背景调查并签署保密协议，委托方定期对受托方人员开展安全审查；
e） 受托方应定期向委托方反馈数据安全评估及审查报告，并根据委托方的意见进行优化改进。

7 政务数据处理安全技术要求

7.1 数据收集

本项要求包括：
a） 数据收集设施应具备数据分类分级能力，并根据政务数据分类分级规范对收集到的政务数据进行数据分类分级；
b） 数据收集设施应具备数据加密存储的能力，可以对收集的数据和缓存数据进行加密存储，并能够对缓存数据进行清除；
c） 当收集的数据传输给其他业务系统时，应进行身份鉴别，满足数据收集的合规性要求和传输安全性要求；
d） 数据收集设施应对所收集数据的数据源进行身份鉴别，满足数据源的真实性要求；
e） 数据收集设施应具备数据校验的能力，满足收集数据的完整性要求；
f） 数据收集设施应具备记录数据收集过程的能力，满足数据收集过程可审计、可追溯；
g） 数据收集设施应具备针对超规模、超范围数据收集行为的告警能力，满足数据收集最小必要原则；
h） 应定期评估数据收集的范围、流程、频次、渠道、方式等，满足数据收集操作的合规性、正当性和一致性要求；

i） 政务数据处理者收集数据前，应对网络服务的性能进行评估，选择可接受的对网络服务影响最小的方式。

7.2 数据存储

本项要求包括：

a） 数据存储设施（包括数据库、云存储系统、大数据平台等）应具有备份机制，应定期核验备份数据的完整性和可用性等，并检查业务数据、备份数据、日志数据等各类数据的存储时限，满足数据存储的时效性要求；
b） 数据存储设施应具有安全隔离及授权管理措施，满足不同进程/工具/应用系统只能访问合法授权数据的要求；
c） 数据存储设施应具备身份鉴别、权限控制、日志审计、数据加密等措施；
d） 数据存储设施应根据待存储数据的类别和级别，执行相应的数据安全保护措施，如敏感个人信息和重要数据应加密存储；
e） 应建立数据存储设施操作的安全控制机制，包括统一身份认证、账号权限最小配置、数据脱敏、操作日志记录与审计等；
f） 应基于密码技术提供重要数据的机密性保护；
g） 应基于密码技术提供政务数据的完整性保护；
h） 政务数据的存储设施应部署于安全区域内，与公共信息网络进行隔离；
i） 应明确政务数据存储安全策略和操作规程，包括政务数据存储设施的安全存储保护措施、数据存储介质安全管控策略和管理规定等；
j） 政务数据应存储于中华人民共和国境内，确需出境应符合国家法律、行政法规和有关规定要求。

7.3 数据使用与加工

7.3.1 系统安全

本项要求包括：

a） 应根据待处理数据的类别和级别，执行相应的数据安全保护措施；
b） 应对数据处理过程进行日志记录，保证数据处理过程可审计、可追溯；
c） 应明确数据使用与加工的流程，包括处理目的、处理方式、应用场景等，并对数据使用与加工流程进行存证，实现数据处理全过程审计。

7.3.2 数据接口安全

本项要求包括：

a） 应采用密码技术保障数据接口传输数据的安全；
b） 应采用数据签名、多因素等技术提供细粒度的身份鉴别和访问控制；
c） 应根据数据应用方唯一标识进行应用身份鉴别、状态校验和权限控制等，对数据接口进行安全管理；
d） 应建立数据接口安全控制策略，明确规定使用数据接口的安全限制条件和安全控制措施，如身份鉴别、授权策略、访问控制、数字签名、时间戳、安全协议、白名单制等；
e） 应采用数据接口参数过滤、限制等措施，防止接口特殊参数注入；
f） 应对数据接口调用日志进行分析，从访问用户、访问频率、访问时间、访问数据量等维度进行数据接口调用行为分析画像，通过告警和阻断机制对异常事件进行实时通知和阻断；

g） 应建立数据接口资产管控和监测审核机制，对数据接口进行资产化管理，对通过数据接口进行交换的的数据进行安全监测和审核。

7.4 数据传输

本项要求包括：

a） 应部署安全通道、采用数据加密等措施，满足数据传输过程的机密性要求；
b） 应具备断点续传、超时重新连接等能力，保障数据传输任务的可靠性；
c） 数据传输设施应依据政务数据分类分级安全策略，执行相应的数据安全保护措施，如敏感个人信息和重要数据加密传输；
d） 应对数据传输过程进行日志记录，满足数据传输过程可审计、可追溯要求。

7.5 数据提供

7.5.1 基础安全

本项要求包括：

a） 数据提供前应对数据提供双方进行身份鉴别，确保数据提供双方身份的合法性；
b） 数据提供设施应根据待提供数据的类别和级别，执行相应的数据安全保护措施，如数据加密、数据脱敏、数字水印等；
c） 数据提供设施应具备身份鉴别、权限控制、日志审计、数据加密、补丁升级等安全防护能力；
d） 数据提供设施应对数据提供过程进行日志记录，满足数据提供过程可审计、可追溯要求。

7.5.2 数据共享

本项要求包括：

a） 数据共享的安全技术措施应遵循 GB/T 39477-2020 的规定；
b） 对通过文件共享协议进行的数据共享，应采用 SFTP 等安全协议，并采取包括共享数据加密、共享前双方身份鉴别、共享过程日志记录等安全措施；
c） 对通过数据共享设施等进行的数据共享，数据共享设施应提供合理的安全措施，包括管理人员权限控制、共享设施缓存数据安全控制、共享设施日志审计、共享设施数据安全风险控制等；
d） 对通过移动硬盘等介质离线拷贝进行的数据共享，应采取包括制定数据存储介质安全管理措施、共享数据加密、共享完成后存储介质中的数据销毁、共享过程日志记录等安全措施；
e） 对通过第三方私有协议或定制开发对接等方式进行的数据共享，应采取包括共享数据加密、共享前双方身份鉴别、共享过程日志记录等安全措施；
f） 应基于数据分类分级规范和数据分类分级安全策略对共享数据进行内容识别和安全管控。

7.6 数据公开

本项要求包括：

a） 应建立数据公开目录，明确数据公开对象；
b） 应在数据公开前，对待公开数据进行内容检查，及时识别并避免重要数据、敏感个人信息的数据公开；
c） 应采用技术手段建立数据溯源能力，并采用校验技术或密码技术保护溯源数据的完整性；
d） 应建立政务数据公开监督机制，对公开数据质量、安全管理工作等进行监督。

7.7 数据销毁

本项要求包括：

a) 应建立不可逆数据删除机制，配置必要的数据删除工具，能根据业务场景需求以不可逆方式删除相关的数据及其衍生的各种副本数据；
b) 应建立物理删除和逻辑删除的数据删除方法和技术，明确不同类别和级别的数据删除方式和安全要求；
c) 应按照法律法规要求，建立数据删除安全操作规范，建立重要数据或个人信息多级级联删除操作模式，明确数据安全删除的操作规程；
d) 应对介质访问、使用、销毁等过程进行记录和审计，并定期对销毁记录及介质销毁效果进行检查。

8 处理政务数据中的个人信息的保护要求

8.1 政务数据中的个人信息主体权利保障

本项要求包括：

a) 政务数据中的个人信息如果收集自第三方（如企事业单位等），应由第三方落实个人信息主体权利保障，处理政务数据的设施应确保与第三方的个人信息保持实时同步；
b) 政务数据中的个人信息收集自个人信息主体，应以清晰易懂语言通过合理渠道向个人信息主体告知数据收集的目的、方式、范围及个人信息处理者名称、联系方式、个人信息保存期限、个人行使法定权利的方式和程序等，并获取个人信息主体授权同意；
c) 政务数据处理设施应提供个人信息撤回机制，对于同意个人信息主体撤回的，应立即停止对其个人信息的处理行为，并对要求撤回的个人信息进行清除。

8.2 政务数据处理设施个人信息安全保护

本项要求包括：

a) 应自动识别个人信息和敏感个人信息，对个人信息和敏感个人信息进行保护，相关措施应遵循GB/T 35273-2020；
b) 收集的个人信息仅限政务数据处理设施对应的政务业务所需，对于政务业务不涉及的个人信息不予收集；
c) 委托其他单位进行政务数据处理时涉及对个人信息的处理，应与委托单位约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务，并对委托人的个人信息处理活动进行监督。

9 政务数据处理安全运营要求

本项要求包括：

a) 应对政务数据处理者在法律法规方面的合规要求进行评估，评估涉及组织、人员、制度与技术等，并对政务数据处理过程的持续合规工作进行检查；
b) 应定期对政务数据处理所涉及的政务数据及关键数据处理设施（如数据库和大数据平台等数据存储载体、数据业务应用、数据分析工具等）开展政务数据处理安全评估，评估方法与评价指标可参考附录 A；

c) 应对政务数据处理相关的数据安全事件和风险信息进行监控，重点对数据异常、数据访问行为异常等进行分析与监测，对于发现的各类数据安全事件及风险进行预警通报，并通过即时通讯、邮件等方式通知相关责任人进行核实及处置；
d) 应对发现的各类数据安全事件采取应急处置措施，包括分析攻击影响面、配置安全策略阻断攻击、修复攻击所利用的安全漏洞等，同时应定期组织应急演练；
e) 应采用技术工具等对于已经发生的各类数据安全事件进行数据安全溯源分析，溯源的目标应包括发现发起攻击的初始源头、攻击进入政务数据处理设施的完整路径，对于溯源分析发现的安全漏洞及隐患应进行及时修复等处置措施；
f) 应定期或基于事件触发等方式，对政务数据处理所有相关的数据安全日志进行审计，审计重点面向数据安全操作是否有泄露、篡改或损坏数据的可能、数据处理活动是否存在异常等，对于发现风险的数据安全日志，应进一步分析及核实数据安全隐患及采取相应的处置措施。

10 政务数据处理安全监督要求

本项要求包括：
a) 应对政务数据处理者的数据收集、存储、使用与加工、传输、提供、共享、公开、销毁等政务数据处理活动进行监督，定期开展政务数据安全合规检查，保障政务数据处理安全合规；
b) 针对重大紧急安全事件，应采取有效措施上报上级主管部门，并同步实施安全事件的分析研判和应急处置；
c) 应建立政务数据安全投诉、举报渠道及受理处置规程，并公布投诉举报方式等信息，及时受理政务数据处理相关的数据安全和个人信息保护投诉举报。

附 录 A
（资料性）
政务数据处理安全评估方法与评价指标

A.1 政务数据处理安全评估方法

A.1.1 明确评估目标

根据政务数据处理相关业务发展情况及数据安全相关法律法规的要求，梳理政务数据处理活动的安全防护现状，找出政务数据处理活动潜在的数据安全风险，并提出政务数据处理安全改进建议。

A.1.2 确定评估范围

根据政务数据处理的评估目标，明确政务数据处理涉及的数据应用平台、数据管理平台等相关系统设施，以及相对应的委托、运营、监督等内外部组织和责任人员。

A.1.3 确定评估方法

评估方法主要包括：

a) 人员访谈：通过访谈的方式与相关责任人员、专职人员、委托方等进行交流，了解制度规章、防护措施、安全责任等方面的落实情况；
b) 文档查验：由被评估方提供数据安全相关的文档材料（如数据安全的方针政策、制度规范流程、培训教育材料，以及产品技术相关的设计实施方案、配置说明、运行记录和其他配套表单等），评估工作组查验相关的文档材料是否已涵盖完整数据生命周期的过程域和控制项；
c) 安全核查：根据被评估方提供的技术材料，登录相关的系统设施，核查其安全策略、配置、防护措施情况；
d) 技术检测：采取测试工具、渗透测试等技术手段对被评估系统的权限管理策略、漏洞修复策略、身份鉴别管理策略、授权访问控制策略等措施是否完备有效进行检测；
e) 抽样检测：从被评估对象中抽取一定比例进行评估，并根据评估结果判断整体数据安全能力情况。该方法适用于被评估对象数量巨大的情形，抽样应考虑抽样随机性及抽样比例，确保抽样结果具有代表性。

A.1.4 执行评估工作

评估具体执行的工作主要包括：

a) 评估信息调研：评估工作组先期开展政务数据处理评估调研，调研内容包括但不限于：数据处理者情况、数据资产情况、数据安全人员情况、数据委托处理情况、数据应用系统情况、数据处理活动情况、安全防护措施情况等；
b) 评估工作准备：评估工作组根据评估目标、评估范围和调研情况，准备评估工作所需的相关材料，调研内容包括但不限于：选取适用依据、确定评估内容、制定评估计划、编制评估方案、被评估方认可授权等；
c) 评估工作实施：评估工作组依照被评估方认可的评估方案实施评估工作，召集被评估方相关责任人员、专职人员和委托方人员召开评估启动会议，采取人员访谈、文档查验、安全核查等方法，基于评价指标逐一核查政务数据处理所涉及的政务数据及关键数据处理设施的安全风险情况，进行安全风险分析和评价，并将获得的各项结果进行准确记录，同时保存相关的证据；
d) 评估报告输出：评估工作组基于现场评估记录的结果和相关证据，编制政务数据处理安全评估

报告，评估报告需要体现政务数据处理所涉及的政务数据及关键数据处理设施的安全现状，并针对存在的风险问题提出改进建议；

e) 评估工作总结：评估工作组召集被评估方相关责任人员、专职人员和委托方人员召开评估总结会议，相关方人员共同确认评估结论是否符合现状、评估结论是否准确、评估报告内容描述是否无误等。

A.2 政务数据处理安全评价指标

政务数据处理安全评价指标涵盖了安全管理要求、安全技术要求、个人信息保护要求、安全运营要求和安全监督要求，共五个部分。

政务数据处理安全评价指标应根据评估对象和范围进行指标选取，选取适用的指标项，对不适用指标项进行说明。其中，对敏感个人信息和重要数据的处理活动要求，设置政务数据处理活动高危风险项，若此类指标项评估为不符合，则直接导致政务数据处理安全评估结论为不合格。

政务数据处理安全评价指标及分值建议如表1所示：

表A.1 政务数据处理安全评价指标

一级指标	二级指标	三级指标	指标说明	分值建议	
安全管理要求	安全组织要求	组织架构	是否明确了政务数据处理的组织架构，并成立数据安全领导小组，负责数据安全统筹规划和组织协调工作；	2	3
		岗位职责	是否分别在决策层、管理层、执行层和监督层明确了责任人员和专职人员，并制定相应的岗位职责；	1	
	安全制度要求	数据安全管理制度	是否制定了政务数据处理的数据安全管理制度，以及建立相应的组织保障机制；	1	12
		数据安全责任人员	是否任命了政务数据处理的数据安全负责人，并将负责人的姓名、联系方式等报送给相关主管部门； 若处理个人信息达到国家网信部门规定数量，是否任命了个人信息保护负责人，并将负责人的姓名、联系方式等报送给相关主管部门；	2	
		数据分类分级规范	是否制定了政务数据处理的数据分类分级规范，明确政务数据的类别和级别，并识别个人信息、敏感个人信息和重要数据；	1	
		数据安全管理规范	是否制定了针对政务数据处理的数据安全管理规范，明确基于数据分类分级的安全管理措施，以及数据访问授权及审批机制等；	1	
		个人信息安全管理规范	是否制定了政务数据处理的个人信息安全管理规范，明确个人信息、敏感个人信息的安全管理措施等；	1	

一级指标	二级指标	三级指标	指标说明	分值建议	
		数据安全运维规范	是否制定了政务数据处理的安全运维规范，明确数据安全风险监测、数据安全应急处置、数据安全风险评估、数据安全审计、数据备份恢复等；	1	
		制度规范审核修订	是否定期审核更新相关的政务数据安全管理制度和规范； 是否具有审核、修订、更新等记录文件；	1	
		数据安全教育培训	是否定期（每年）开展政务数据处理安全教育培训，并依据培训反馈效果定期对教育培训计划进行审核和更新；	1	
		政务数据安全报告	是否制定了政务数据处理的安全报告制度，明确数据安全事件报告及数据安全风险评估报告等制度要求；	1	
		等级保护安全管理	处理政务数据的信息系统，是否按照网络安全等级保护基本要求开展防护，并遵循《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》对应的级别要求；	1	
		密码应用安全管理	处理政务数据的信息系统，是否制定了密码安全应用管理制度，并遵循《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》对应的级别要求；	1	
	第三方安全要求	委托方审批监督	是否存在委托他人建设、维护政务数据处理设施并处理政务数据的情形； 若存在，受托方是否经过严格审批程序进行选择，是否对受托方履行政务数据处理安全要求的情况进行监督；	2	6
		受托方合规责任	受托方是否存在留存、使用或者向他人提供政务数据的情形； 若存在，受托方的操作行为是否符合法律法规的规定和合同约定，获得相应授权同意；	1	
		受托方安全责任	受托方是否明确知悉委托活动中涉及的重要数据和个人信息的类别和安全级别，并予以重点保护； 受托方是否建立组织保障机制以保证数据处理的安全； 委托方是否建立相应的组织保障监督职责；	1	
		受托方人员责任	受托方是否建立人员安全管理制度，明确人员安全管理中各环节的操作规程； 受托方参与政务数据处理的人员是否进行了必要的背景调查，是否签署了保密协议； 委托方是否定期对受托方的人员开展审查；	1	

一级指标	二级指标	三级指标	指标说明	分值建议	
		受托方评估审查	受托方是否定期向委托方反馈数据安全评估及审查报告的情况； 委托方是否提出意见以便受托方进行优化改进；	1	
安全技术要求	数据收集	数据收集合规性	收集的数据传输给其他业务系统时，是否进行身份鉴别； 数据收集是否满足合规性要求和传输安全性要求；	1	9
		数据收集真实性	数据收集设施是否对所收集数据的数据源进行身份鉴别，是否满足数据源的真实性要求；	1	
		数据收集完整性	数据收集设施是否具备数据校验的能力，是否满足收集数据的完整性要求；	1	
		数据收集合规要求	数据收集设施是否具备针对超规模、超范围数据收集行为的告警能力，是否满足数据收集最小必要原则； 是否定期对数据收集操作进行评估，评估其是否满足数据收集操作的合规性、正当性和一致性要求；	2	
		数据收集性能评估	在政务数据处理者收集数据前，是否对网络服务的性能进行评估，选择可接受的对网络服务影响最小的方式；	1	
		收集设施分类分级	数据收集设施是否具备数据分类分级能力； 是否根据政务数据分类分级规范对收集到的政务数据进行数据分类分级；	1	
		收集设施加密存储	数据收集设施是否具备数据加密存储能力； 是否对收集的数据和缓存数据进行加密存储； 是否对缓存数据进行清除；	1	
		收集设施审计追溯	数据收集设施是否具备记录数据收集过程的能力； 是否满足数据收集过程可审计、可追溯；	1	
	数据传输	数据传输机密性	是否部署安全通道、采用数据加密等措施，满足数据传输过程的机密性要求；	2	7
		数据传输完整性	是否部署安全通道、采用数据加密等措施，满足数据传输过程的完整性要求；	2	
		数据传输可靠性	是否具备断点续传、超时重新连接等能力，保障数据传输任务的可靠性；	1	
		数据传输审计追溯	是否对数据传输过程进行日志记录，满足数据传输过程可审计和可追溯的要求；	1	

一级指标	二级指标	三级指标	指标说明	分值建议	
		传输设施分类分级	数据传输设施是否依据政务数据分类分级安全策略，执行相应的数据安全保护措施；	1	
	数据存储	存储设施授权控制	数据存储设施是否具有安全隔离及授权管理措施，满足不同进程/工具/应用系统只能访问合法授权数据的要求； 是否建立了数据存储设施操作的安全控制机制，支持统一身份认证、账号权限最小配置等；	1	12
		存储设施安全隔离	政务数据的存储设施是否部署于安全区域内，与公共信息网络进行隔离；	1	
		存储设施能力要求	数据存储设施是否具备身份鉴别、权限控制、日志审计、数据加密、补丁升级等能力；	1	
		数据存储备份机制	数据存储设施是否具有备份机制，并定期核验备份数据的完整性和可用性； 是否定期检查各类数据的存储时限，满足数据存储的时效性要求；	2	
		数据存储分类分级	数据存储设施是否根据待存储数据的类别和级别，执行相应的数据安全保护措施；	1	
		重要数据机密性	是否提供了基于密码技术的重要数据机密性保障手段，针对重要数据的机密性进行保护；	2	
		政务数据完整性	是否提供了基于密码技术的政务数据完整性保障手段，针对政务数据的完整性进行保护；	1	
		政务数据安全策略	是否明确了政务数据存储安全策略和操作规程，包括政务数据存储设施的安全存储保护措施、数据存储介质安全管控策略和管理规定等；	1	
		政务数据存储位置	政务数据是否存储于中华人民共和国境内； 确需出境的情形，是否符合国家法律、行政法规和有关规定要求；	2	
	数据使用加工	数据处理保护措施	是否根据待处理数据的类别和级别，执行相应的数据安全保护措施；	1	
		数据处理机密性	是否采用密码技术对数据进行加密，保障数据在使用加工过程中的机密性；	1	

一级指标	二级指标	三级指标	指标说明	分值建议	
		数据处理审计追溯	是否明确了数据使用与加工的流程，并对数据处理过程进行日志记录，保证数据处理全过程可审计和可追溯；	1	
		数据 API 监测审核	是否建立 API 资产管控和监测审核机制，对通过 API 进行交换的数据进行安全监测和审核；	1	8
		数据 API 传输通道	是否采用密码技术保障 API 数据传输通道的安全；	1	
		数据 API 鉴别控制	是否采用数据签名或加密技术提供细粒度的身份鉴别和访问控制； 是否根据数据应用方唯一标识进行应用身份鉴别、状态校验和权限控制等，对数据 API 进行安全管理；	1	
		数据 API 限制策略	是否建立数据 API 安全控制策略，明确规定使用数据 API 的安全限制条件和安全控制措施； 是否采用数据 API 参数过滤、限制等措施，防止接口特殊参数注入；	1	
		数据 API 分析阻断	是否对数据 API 调用日志进行分析，通过告警和阻断机制对异常事件进行实时通知和阻断；	1	
	数据提供	数据提供身份鉴别	数据提供前是否对数据供需双方进行身份鉴别，确保数据供需双方身份的合法性；	1	
		数据提供分类分级	数据提供设施是否根据待提供数据的类别和级别，执行相应的数据安全保护措施；	1	
		提供设施安全能力	数据提供设施是否具备身份鉴别、权限控制、日志审计、数据加密、补丁升级等安全防护能力；	1	
		提供设施审计追溯	数据提供设施是否对数据提供过程进行日志记录，满足数据处理过程可审计和可追溯要求；	1	
		数据共享技术要求	数据共享的安全技术措施是否遵循《GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求》的规定； 对通过文件共享协议进行的数据共享，是否采用 SFTP 等安全协议，是否采取包括共享数据加密、共享前双方身份鉴别、共享过程日志记录等安全措施；	1	8
		共享设施安全措施	通过数据共享设施等进行的数据共享，数据共享设施是否提供合理的安全措施；	1	

一级指标	二级指标	三级指标	指标说明	分值建议	
			通过第三方私有协议或定制开发对接等方式进行的数据共享，是否采取合理的安全措施；		
		数据共享分类分级	是否基于数据分类分级规范对共享数据进行内容识别和安全管控；	1	
		离线共享安全措施	通过移动硬盘等介质离线拷贝进行的数据共享，是否采取合理的安全措施；	1	
	数据公开	数据公开目录	是否建立了数据公开目录，是否明确了数据公开对象；	1	5
		数据公开前置检查	在数据公开前，是否对待公开数据进行内容检查，识别并停止重要数据、敏感个人信息的数据公开；	2	
		数据溯源	是否采用技术手段建立数据溯源能力，并采用校验技术或密码技术保护溯源数据的完整性；	1	
		数据公开监督	是否建立政务数据公开监督机制，对公开数据质量、安全风险、安全管理工作等进行监督；	1	
	数据销毁	不可逆数据删除	是否建立了不可逆的数据删除机制，配置必要的数据删除工具，能根据业务场景需求以不可逆方式删除相关的数据及其衍生的各种副本数据；	1	4
		数据删除方法技术	是否建立物理删除和逻辑删除的数据删除方法和技术； 是否明确不同类别和级别的数据删除方式和安全要求；	1	
		数据删除操作规范	是否按照法律法规要求，建立数据删除安全操作规范，建立重要数据或个人信息多级联删除操作模式，明确数据安全删除的操作规程；	1	
		数据删除审计监督	是否对介质访问、使用、销毁等过程进行记录和审计，并定期对销毁记录及介质销毁效果进行检查；	1	
个人信息保护要求	个人信息主体权利保障	第三方设施收集	政务数据中的个人信息是否收集自第三方设施； 若收集自第三方设施，第三方设施是否落实了个人信息主体权利保障； 处理政务数据的设施是否与第三方设施的个人信息保持实时同步；	1	4
		个人信息主体权利	政务数据中的个人信息是否收集自个人信息主体；	2	

一级指标	二级指标	三级指标	指标说明	分值建议	
			若收集自个人信息主体，是否以清晰易懂语言通过合理渠道向个人信息主体告知数据收集的目的、方式、范围及个人信息处理者名称、联系方式、个人信息保存期限、个人行使法定权利的方式和程序等，并获取个人信息主体授权同意； 是否依据《GB/T 35273-2020 信息安全技术 个人信息安全规范》保障落实个人信息主体的权利； 是否有措施保障已死亡的个人信息主体的权利落实；		
		个人信息撤回机制	政务数据处理设施是否提供了个人信息撤回机制； 对于同意个人信息主体撤回的，是否可立即停止对其个人信息的处理行为，并对要求撤回的个人信息进行清除；	1	
	政务数据处理设施个人信息安全保护	个人信息分类分级保护	政务数据处理设施是否具备自动识别个人信息和敏感个人信息的能力； 相关措施是否遵循《GB/T 35273-2020 信息安全技术 个人信息安全规范》的相关要求； 是否依据《GB/T 41817-2022 信息安全技术 个人信息安全工程指南》为涉及个人信息处理的网络产品和服务（含信息系统）开展同步规划和同步建设；	1	4
		个人信息收集必要	政务数据处理设施所收集的个人信息是否为对应政务业务所必需；	2	
		个人信息委托监督	组织是否存在委托其他单位进行政务数据处理时涉及对个人信息的处理； 若存在，是否与委托单位约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务，是否对委托单位的个人信息处理活动进行监督；	1	
安全运营要求	安全合规评估	安全合规评估	是否定期（每年）对政务数据处理者在法律法规方面的合规要求进行评估，评估报告是否能够保存三年以上； 是否对政务数据的处理过程进行持续性合规检查；	1	13
	安全风险评估	安全风险评估	是否定期（每年）对政务数据处理所涉及的政务数据及关键数据处理设施开展政务数据处理安全评估，评估报告是否能够保存三年以上；	2	

一级指标	二级指标	三级指标	指标说明	分值建议	
			是否对政务数据处理所涉及的政务数据及关键数据处理设施开展持续性安全检查；		
	安全风险监控	监控要点	是否对政务数据处理相关的数据安全事件和风险信息进行监控，对各类异常行为进行监测分析；	1	
		通报处置	是否对发现的各类数据安全事件及风险进行预警通报，并通过即时通讯的方式通知相关责任人进行核实及处置；	1	
	安全事件应急响应	处置措施	是否发生过数据安全事件； 是否具备数据安全事件采取应急处置的能力；	1	
		应急演练	是否定期（每年）组织数据安全事件的应急演练；	2	
	安全溯源分析	溯源分析	是否采用技术工具等对于已经发生的各类数据安全事件进行数据安全溯源分析，能够发现发起攻击的初始源头、攻击进入政务数据处理平台的完整路径；	1	
		修复处置	是否有能力对于溯源分析发现的安全漏洞及隐患应进行及时修复等处置措；	1	
	安全日志审计	日志审计	是否定期或基于事件触发等方式，对政务数据处理所有相关的数据安全日志进行审计；	2	
		分析处置	是否对于发现风险的数据安全日志，进行分析及核实数据安全隐患及采取相应的处置措施；	1	
安全监督要求	监督合规检查	监督合规检查	是否对政务数据处理者在各环节的政务数据处理活动进行监督； 是否定期开展政务数据安全合规检查；	1	5
	重大安全事件应急	重大安全事件应急	是否建立重大紧急安全事件的有效处置及上报机制； 是否具备重大紧急安全事件同步实施研判和应急处置的能力；	2	
	投诉举报机制	投诉举报	是否建立了政务数据安全投诉、举报渠道及受理处置规程，并公布投诉举报方式等信息；	1	
		受理处置	是否具备及时受理政务数据处理相关的数据安全和个人信息保护投诉举报的能力。	1	

参 考 文 献

[1] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国网络安全法.2016年11月7日.

[2] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国密码法.2019年10月26日.

[3] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国数据安全法.2021年6月10日.

[4] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国个人信息保护法.2021年8月20日.

[5] 中华人民共和国国务院.关键信息基础设施安全保护条例.2021年7月30日.