ICS 35.030
CCS L 70

T/CSAS

团　　体　　标　　准

T/CSAS 0010—2025

政务数据处理安全要求

Government data processing security requirements

2025-05-23 发布　　2025-07-01 实施

四川省网络空间安全协会　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：成都久信信息技术股份有限公司、成都理工大学、全域数据信息安全重点联合实验室西南实验室。

本文件主要起草人：李阳冬、朱光剑、张傑、李冬芬、吴旭、曹吉锋、田茂呈（排名不分先后）。

政务数据处理安全要求

1 范围

本文件规定了电子政务数据分级的原则、方法，以及政务数据的安全保护、通用安全要求、技术要求和管理要求。

本文件适用于各级政务部门在政务数据收集、传输、存储、处理、加工、共享、开放、使用、销毁等全生命周期的分级安全防护，也适用于网络安全主管部门对政务数据安全保护的监督管理。

本文件不适用于涉及国家秘密信息的政务数据。

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 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 28448 信息安全技术 网络安全等级保护测评要求

GB/T 28449 信息安全技术 网络安全等级保护测评过程指南

GB/T 38664.1 信息技术 大数据 政务数据开放共享 第1部分：总则

GB/T 41479 信息安全技术 网络数据处理安全要求

DB11/T 1918 政务数据分级与安全保护规范

DB51/T 3058 政务数据 数据脱敏规范

T/CSAS 0001—2025 数据生命周期安全参考框架

3 术语和定义

GB/T 38664.1—2020、T/CSAS 0001—2025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。

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

[来源：GB/T 38664.1—2020，3.1]

3.2

数据全生命周期处理活动 data lifecycle processing activities

数据生命周期过程中发生的各项数据处理活动，包括：数据的收集、存储、使用、加工、传输、提供、公开、销毁等。

[来源：T/CSAS 0001—2025，3.7]

3.3

数据脱敏处理 data masking

对个人信息和重要数据通过脱敏规则进行数据变形处理，降低其敏感程度。

3.4

数据加密　data encryption

通过加密算法和加密密钥将明文转变为密文的过程。

3.5

数据处理活动　data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、销毁等活动。

4　数据分级

4.1　分级原则

4.1.1　分级管控原则

通过对数据进行分级，推动建立基于分级的数据全生命周期安全防护体系，确保在安全可控的环境下，促进数据共享和开放。

4.1.2　实用性原则

政务数据分类应从基础库建设及政务数据应用等实际需求出发，确保各个类目下都含有真实、有价值的数据，不设定无价值类目，设定的数据类目符合普遍认知且综合实用。

4.1.3　扩展性原则

政务数据分类保证类目的可扩展性、兼容性，可适应未来阶段政府部门机构调整、经济发展变化、基础库建设规划调整导致的类目增减和数据类型变化等情况。

4.2　分级因素

4.2.1　因素构成

数据分级基于分级因素进行综合判定，分级因素包括：数据发生泄露、篡改、丢失或滥用后的影响对象和影响范围。

4.2.2　影响对象

数据发生泄露、篡改、丢失或滥用后的影响对象包括国家安全、社会秩序及公共利益、政府机构、企事业单位及其他社会组织自身权益或者个人权益，具体如下：

a）　国家安全，包括国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力；

b）　社会秩序及公共利益，包括医疗卫生、生产经营、教学科研、公共环境、市政项目、文体旅游、社会福利、住宅用房及其他公用事业等社会秩序和公众的身心健康、政治权利、人身自由、经济权益等；

c）　政府机构、企事业单位及其他社会组织自身权益，包括某政府机构、企事业单位或其他社会组织的生产经营、声誉形象、公信力、资金资产等；

d）　个人权益，包括个人的隐私、财产、生命安全、精神、名誉以及私人活动和领域等。

4.2.3　影响程度

数据发生泄露、篡改、丢失或滥用后的影响程度包括一般影响、严重影响和特别严重影响，具体描述见表1。

表 1　影响程度

程度	定义
一般影响	数据发生泄露、篡改、丢失或滥用后对国家安全、社会秩序及公共利益、政府机构、企事业单位及其他社会组织自身权益及个人权益等造成一般损害。
严重影响	数据发生泄露、篡改、丢失或滥用后对国家安全、社会秩序及公共利益、政府机构、企事业单位及其他社会组织自身权益及个人权益等造成严重损害。
特别严重影响	数据发生泄露、篡改、丢失或滥用后对国家安全、社会秩序及公共利益、政府机构、企事业单位及其他社会组织自身权益及个人权益等造成特别严重损害。

4.3　分级描述

综合考虑数据发生泄露、篡改、丢失或滥用后的影响对象、影响程度，将数据划分为四级，具体描述见表2。

表 2　数据分级矩阵表

影响对象	影响程度		
	一般影响	严重影响	特别严重影响
个人权益	一级	二级	二级
政府机构、企事业单位及其他社会组织自身权益	二级	三级	三级
社会秩序及公共利益	二级	三级	四级
国家安全	三级	四级	四级
注：当社会秩序及公共利益遭受侵害且可能影响国家安全时，优先考虑对国家安全的影响程度。社会秩序及公共利益严重影响对应国家安全一般影响，以此类推。			

5　政务数据安全保护要求

5.1　通用安全要求

5.1.1　身份鉴别

处理政务数据的信息系统身份鉴别应满足以下安全要求：

a) 对登录信息系统的用户，应采用“用户名+口令”等认证方式，进行身份鉴别（适用等级：一级）；

b) 对登录信息系统的用户，应采用“用户名+口令”和“动态口令”、“用户名+口令”和“数字证书认证”、“用户名+口令”和“人脸识别等生物特征认证”等组合认证方式，进行身份鉴别（适用等级：二级）；

c) 对登录信息系统的用户，应采用“用户名+口令”和“数字证书实名认证”、“用户名+口令”和“人脸识别等生物特征认证”等组合认证方式，进行身份鉴别（适用等级：三级及以上）；

d) 应建立统一的身份认证机制，对系统用户实现统一身份管理（适用等级：二级及以上）；

e) 对系统用户的登录应有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施（适用等级：一级及以上）；

f) 应针对重要操作或个人信息、敏感数据、重要数据的访问建立技术管理者多方认证机制（适用等级：三级及以上）。

注：数据分级后的安全要求参照各条款后的适用等级进行衡量，适用等级越高，安全要求越严格。如标注“适用等级：一级”的条款，适用于一级数据的安全要求，以此类推。

5.1.2 访问控制安全

处理政务数据的信息系统访问控制应满足以下安全要求：

a) 应建立基于主体角色授权的访问控制（适用等级：一级）；
b) 应建立基于主体角色授权的访问控制，并在此基础上建立基于客体属性授权的访问控制（适用等级：二级及以上）；
c) 应建立基于共享、开放任务授权的访问控制，应设置访问权限有效期，在共享、开放任务结束后及时收回权限（适用等级：二级及以上）；
d) 应赋予操作主体最小操作权限和最小数据集，并实现管理用户的权限分离（适用等级：三级及以上）；
e) 应制定数据访问授权审批流程，对数据活动主体的操作权限和范围变更制定申请和审批流程（适用等级：三级及以上）；
f) 应实现基于认证机制的权限控制，根据用户认证方式合理设置相匹配的访问权限（适用等级：三级及以上）；
g) 应建立统一数据出口访问控制管理机制，对数据共享、开放及使用等（包括但不限于：数据服务接口、数据文件等方式）进行统一审核管理、监控留痕和统一出口管控，依申请对数据内容、提供形式、频率、周期等进行审核，在审核确认后，按共享或开放授权范围予以提供（适用等级：三级及以上）。

5.1.3 数据标识安全

处理政务数据的信息系统数据标识应满足以下安全要求：

a) 应标识数据的级别、共享属性、开放属性（适用等级：一级及以上）；
b) 应能在数据存储、加工、共享、开放、使用等过程中识别数据的标识（适用等级：二级及以上）；
c) 应采取技术手段对数据资产进行管理（适用等级：三级及以上）。

5.1.4 安全审计

处理政务数据的信息系统安全审计应满足以下安全要求：

a) 应对数据收集、存储、加工、分析、共享、开放、使用等处理环节的操作行为建立日志，日志的内容包括但不限于：时间、IP地址、用户ID、操作内容、操作对象等（适用等级：一级及以上）；
b) 日志保存期限应不少于12个月（适用等级：一级及以上）；
c) 应采取备份等措施对审计日志进行保护，避免未预期的删除、修改或破坏（适用等级：二级及以上）；
d) 应采取技术措施对日志进行审计，对操作异常行为进行识别分析并及时督促整改（适用等级：二级及以上）；
e) 应对审计进程进行保护，防止未经授权的中断（适用等级：三级及以上）；
f) 定期对审计日志进行分析，主动并及时发现安全风险和隐患（适用等级：四级）。

5.1.5 监测溯源

处理政务数据的信息系统监测溯源应满足以下安全要求：

a) 应采取技术措施对数据收集、传输、存储、加工、共享、开放、使用等处理环节进行监测，确

保数据的正当使用（适用等级：一级）；

b) 应采取技术手段实时监控数据收集、传输、存储、加工、共享、开放、使用等过程，及时发现异常行为，防止个人信息、敏感数据和重要数据的泄露、篡改、丢失和滥用（适用等级：二级及以上）；

c) 应实时监控数据交换服务接口的调用信息，分析是否存在恶意数据获取、数据盗用等风险（适用等级：

d) 应实时监控和记录个人信息、敏感数据和重要数据的外发行为，记录交换数据的种类、数量和数据接收方等信息（适用等级：二级及以上）；

e) 应对异常或高风险数据操作行为进行自动化识别和实时预警（适用等级：三级及以上）；

f) 应采取技术手段对数据专区内数据开放过程进行实时监测，并记录和分析监测日志（适用等级：三级及以上）；

g) 应建立数据追踪溯源机制，实现对数据异常流量的实时监测，确保数据在使用过程中来源清晰、去向明确，一旦数据发生泄露、篡改、丢失或滥用，可以通过溯源分析，进行问题溯源追踪（适用等级：二级及以上）。

5.2 技术要求

5.2.1 数据收集安全

处理政务数据的信息系统数据收集应满足以下安全要求：

a) 应明确数据采集来源、采集范围、采集方式、采集周期和频率等，确保数据采集的合法性、必要性、正当性（适用等级：一级及以上）；

b) 部署统一化数据采集工具，设定安全策略（适用等级：二级及以上）；

c) 应依据最小化原则实现采集账号认证及权限分配（适用等级：二级及以上）；

d) 应采取技术手段和管理措施，防止数据采集过程中个人信息、敏感数据和重要数据的泄露、篡改、丢失（适用等级：二级及以上）；

e) 采集个人信息、个人敏感信息时，应征得个人信息主体或其监护人的同意，应确保获得的同意是其在完全知情的基础上自主给出的，有具体、清晰、明确的意愿表示（适用等级：二级及以上）；

f) 采集个人信息、个人敏感信息时，应有明确的法律法规或政策依据，应建立统一、规范的采集流程、采集方式和采集管理机制，避免无秩序、无规则的个人信息、个人敏感信息的滥采乱收（适用等级：二级及以上）；

g) 利用信息系统、网站或APP采集个人信息时，应制定隐私政策等方式明确采集个人信息的目的、类型、安全保护措施等内容，并向个人信息主体提供撤回收集、使用其个人信息授权的方法（适用等级：二级及以上）；

h) 能够通过共享方式获取个人信息的，不应重复采集相应信息（适用等级：二级及以上）。

5.2.2 数据存储安全

处理政务数据的信息系统数据存储应满足以下安全要求：

a) 应提供数据的本地数据备份与恢复功能（适用等级：一级及以上）；

b) 应设置数据存档规则，将暂时不使用的数据进行存档处理（适用等级：一级至三级）；

c) 应设置数据存档规则，将暂时不使用的数据进行存档处理，存档设备应与生产数据所在网络物理隔离（适用等级：四级）；

d) 应加强对存档设备的安全防护，防止敏感信息泄露（适用等级：四级）；

e) 应建立开放可伸缩的存储架构，满足数据量持续增长的需求（适用等级：一级及以上）；

f） 应采用必要的技术和管理措施，确保数据存储的完整性、一致性和可用性（适用等级：一级及以上）；
g） 应采用国家密码管理部门核准的密码技术保证敏感数据在存储过程中的保密性，如SM4-CBC（适用等级：二级至三级）；
h） 应采用国家密码管理部门核准的密码技术保证数据在存储过程中的保密性，如SM4-CBC（适用等级：四级）；
i） 应对不同级别的数据进行隔离存储，并在各自存储区域之间设置严格的访问控制规则（适用等级：二级及以上）；
j） 应提供异地数据备份功能，利用通信网络将数据定时批量传输至备份场地（适用等级：二级至三级）；
k） 应提供异地实时备份功能，利用通信网络将数据实时传输至备份场地（适用等级：四级）；
l） 应设置个人信息存储期限，确保存储期限为实现个人信息使用目的所需的最短时间（适用等级：二级及以上）；
m） 应将去标识化的个人信息与可用于恢复识别个人的信息分开存储（适用等级：三级及以上）；
n） 个人生物识别信息应与其他信息分开存储（适用等级：四级）；
o） 对重要数据存储系统及其安全配置定期扫描，符合系统安全基线要求（适用等级：三级及以上）。

5.2.3 数据传输安全

处理政务数据的信息系统数据传输应满足以下安全要求：
a） 应采用校验技术保证传输过程中数据的完整性，如海明校验码（适用等级：一级至二级）；
b） 应采用密码技术保证传输过程中数据的完整性，如HMAC-SM3（适用等级：三级至四级）；
c） 应采用国家密码管理部门核准的密码技术保证敏感数据在传输过程中的保密性，如SM4算法（适用等级：二级至三级）；
d） 应采用国家密码管理部门核准的密码技术保证数据在传输过程中的保密性，如SM4算法（适用等级：四级）；
e） 数据在以导入/导出方式进行传输时，应对提供方、接收方建立相应的流转记录、签收确认、防抵赖机制，传输过程应使用只读存储介质，并及时销毁导入/导出终端上的临时数据（适用等级：二级及以上）；
f） 应提供重要数据所在系统的热冗余，保证系统数据的高可用性（适用等级：三级及以上）。

5.2.4 数据处理安全

处理政务数据的信息系统数据处理应满足以下安全要求：
a） 应采用具有数据静态脱敏和数据动态脱敏能力的工具，并对脱敏操作过程进行审计并保留审计记录（适用等级：三级及以上）；
b） 应采用实时查询脱敏技术，在实时查询时，仅展示用户权限范围内的数据信息，避免敏感数据泄露，如通过动态字节码技术将脱敏逻辑嵌入应用系统，实时拦截数据请求并处理（适用等级：三级及以上）；
c） 数据库管理员维护生产环境时，应根据权限动态屏蔽敏感字段，防止内部泄露，结合用户身份认证和细粒度脱敏策略，支持“完全脱敏”“部分脱敏”分级控制，如通过代理网关拦截查询请求并改写查询（如拦截SELECT语句并添加脱敏函数）（适用等级：三级及以上）；
d） 在进行敏感数据共享时，应实时脱敏重要敏感字段，确保共享安全性，如通过标准化API或SDK提供脱敏服务，业务系统调用接口实现动态脱敏（适用等级：三级及以上）；
e） 应采用数据分析和使用过程中的日志记录工具，并对分析过程和结果进行安全审查，确定使用

授权流程（适用等级：二级及以上）；

f） 应使用相关技术手段对数据处理过程进行全程监控，必要时进行操作阻断（适用等级：二级及以上）；

g） 应使用对个人身份信息、重要或敏感数据进行处理操作的日志记录工具（适用等级：四级）。

5.2.5 数据共享安全

处理政务数据的信息系统数据共享应满足以下安全要求：

a） 应根据共享方式（包括但不限于：库表交换、导入导出、接口调用、文件提供等）设置数据共享规则，并按照规则执行相应操作（适用等级：一级及以上）；

b） 应能识别出敏感数据或个人敏感信息，并对其进行脱敏后再共享；确需直接对其进行非脱敏的共享时，应获得信息主体的授权同意，经审核批准后予以共享；或进行可用不可见的共享（适用等级：二级至三级）；

c） 只允许进行可用不可见的共享（适用等级：四级）；

d） 应设置严格的访问控制策略，依据权限合理调配数据（适用等级：二级及以上）；

e） 应采取技术手段和管理措施，保证数据在共享过程中的安全，防止个人信息、敏感数据和重要数据的泄露、篡改、丢失及滥用（适用等级：二级及以上）；

f） 应采取技术措施对异常或高风险数据共享行为进行自动化识别和实时预警，对违规行为及时进行阻断（适用等级：四级）；

g） 应仅允许数据在本地导入、导出（适用等级：三级及以上）；

h） 个人信息共享时，应充分重视风险，事先开展个人信息安全影响评估，并采取有效保护个人信息主体的措施（适用等级：一级及以上）；

i） 应采取技术措施保证个人生物识别信息、基因信息的完整性和保密性，严格限制对其进行共享操作（适用等级：四级）。

5.2.6 数据开放安全

处理政务数据的信息系统数据开放应满足以下安全要求：

a） 应仅通过数据专区对外开放数据（适用等级：一级及以上）；

b） 应设置数据专区的访问控制规则，实现基于角色的访问控制（适用等级：一级）；

c） 应设置数据专区的访问控制规则，实现基于角色的访问控制，并在此基础上建立基于属性的访问控制（适用等级：二级及以上）；

d） 应设置数据专区的访问控制规则，应建立基于开放任务授权的访问控制，应设置访问权限有效期，在开放任务结束后及时收回权限（适用等级：二级及以上）；

e） 应根据业务需要，依据开放方式（包括但不限于：库表交换、导入导出、接口调用、文件提供等）设置数据开放规则，并按照规则执行相应操作（适用等级：一级及以上）；

f） 应能识别出敏感数据或个人敏感信息，并对其进行脱敏后再开放；确需直接对其进行非脱敏的开放时，应获得信息主体的授权同意，经审核批准后予以开放，或进行可用不可见的开放（适用等级：二级至三级）；

g） 只允许进行可用不可见的开放（适用等级：四级）；

h） 应采取技术手段和管理措施，保证数据在开放过程中的安全，防止个人信息、敏感数据和重要数据的泄露、篡改、丢失及滥用（适用等级：二级及以上）；

i） 应采取技术措施严格控制数据的访问和使用，仅允许数据在内部处理，防止数据外泄（适用等级：四级）；

j） 应采取技术措施对异常或高风险数据访问行为进行自动化识别和实时预警，对违规行为及时进

行阻断（适用等级：四级）；

k) 涉及公开展示或披露个人信息的，应根据业务需要对个人信息进行必要的去标识化处理，降低信息泄露风险（适用等级：二级及以上）；

l) 应采取技术措施严格限制个人敏感信息的开放操作，仅允许特定对象、特定方式的开放操作（适用等级：三级及以上）。

5.2.7 数据加工安全

处理政务数据的信息系统数据加工应满足以下安全要求：

a) 应设置严格的访问控制规则防止非授权的加工、分析操作（适用等级：一级及以上）；

b) 应明确数据加工、分析的目标和范围，确保加工前后数据映射关系（适用等级：一级及以上）；

c) 应对加工、分析产生的新数据设置级别标签（适用等级：一级及以上）；

d) 远程加工、分析数据时，应严格限制数据加工、分析终端的接入IP数量和地址（适用等级：一级至三级）；

e) 应仅在内部进行数据加工、分析操作，并采取技术措施禁止远程加工、分析数据（适用等级：四级）；

f) 应不在数据加工、分析终端上保存数据（适用等级：一级及以上）；

g) 应能识别出敏感数据或个人敏感信息，并对其进行脱敏后再进行加工、分析，确需直接对其进行非脱敏的加工、分析时，应获得信息主体的授权同意，经审核批准后进行（适用等级：二级至三级）；

h) 应能识别出个人信息、敏感数据和重要数据，脱敏后再进行加工、分析（适用等级：四级）；

i) 应在数据清洗、转换、分析等加工处理过程中对个人信息、敏感数据和重要数据进行保护，避免数据的泄露、篡改、丢失，并在产生问题时能有效还原和恢复（适用等级：二级及以上）；

j) 应防止数据加工、分析过程中的调试信息、日志记录、不受控输出等泄露敏感信息（适用等级：三级及以上）。

5.2.8 数据使用安全

处理政务数据的信息系统数据使用应满足以下安全要求：

a) 针对数据应用的访问，应进行应用身份鉴别和授权处理（适用等级：一级及以上）；

b) 应针对不同级别的数据设置不同的访问权限，不同用户只能访问与自己权限对应的数据（适用等级：二级及以上）；

c) 针对个人信息、敏感数据和重要数据的访问、使用和展示，应根据业务需要进行必要的去标识化或脱敏处理，确需直接对其进行非脱敏的访问、使用和展示时，应获得信息主体的授权同意，经审核批准后予以访问、使用和展示（适用等级：二级及以上）；

d) 针对共享、开放、使用等过程中获得的数据，数据接收、调用方未经允许不得私自本地化留存（适用等级：三级及以上）；

e) 涉及高风险操作时应遵循多人操作管理原则，确保单人无法拥有重要数据的完整操作权限（适用等级：四级）。

5.2.9 数据销毁安全

处理政务数据的信息系统数据销毁应满足以下安全要求：

a) 应使用规范的工具或产品执行数据销毁工作（适用等级：一级及以上）；

b) 应确保以不可逆方式销毁数据及其副本内容（适用等级：二级及以上）；

c) 应采用可靠技术手段销毁个人信息、敏感数据和重要数据，确保信息不可还原（适用等级：二

级及以上）；

d) 对于数据存储介质的销毁，应使用国家权威机构认证的设备对存储介质进行物理销毁（适用等级：三级）；

e) 对于数据存储介质的销毁，应选择具有国家认定资质的销毁服务提供商执行存储介质的销毁工作（适用等级：四级）。

5.3 管理要求

5.3.1 安全策略

处理政务数据的信息系统安全策略应满足以下安全要求：

a) 应制定数据安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等（适用等级：一级及以上）；

b) 应建立数据安全管理策略，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，包括但不限于数据存储策略、数据加解密策略、数据脱敏策略、数据溯源策略、数据导入/导出策略、数据共享开放策略、数据销毁策略等（适用等级：一级及以上）；

c) 应对数据安全管理活动中的主要管理内容建立安全管理制度（适用等级：二级及以上）；

d) 应对管理人员或操作人员执行的日常管理操作建立操作规程（适用等级：三级及以上）；

e) 应制定并执行数据分级保护策略，针对不同级别的数据制定不同的安全保护措施（适用等级：一级及以上）；

f) 应在数据分级的基础上，再对数据（包括但不限于：个人信息、敏感数据和重要数据）进行分类，明确进行脱敏或去标识的使用场景和业务处理流程（适用等级：二级及以上）；

g) 应定期评审数据安全管理制度、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（适用等级：三级及以上）。

5.3.2 安全机构

处理政务数据的信息系统安全机构应满足以下安全要求：

a) 应设立数据安全管理的职能部门，设立数据管理员、安全管理员、系统管理员、审计管理员等负责人岗位，明确部门职能和岗位职责（适用等级：一级及以上）；

b) 应成立指导和管理数据安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权（适用等级：二级及以上）；

c) 应设立数据保护官，负责对个人信息、敏感数据和重要数据进行保护（适用等级：二级及以上）；

d) 应配备专职的数据安全员、安全管理员，且不可兼任（适用等级：四级）；

e) 应明确内部涉及个人信息处理的各岗位安全责任，当发生安全事件时能够进行相应的处罚（适用等级：四级）；

f) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等（适用等级：一级及以上）。

5.3.3 安全人员

处理政务数据的信息系统安全人员应满足以下安全要求：

a) 应指定或授权专门的部门或人员负责人员录用（适用等级：一级及以上）；

b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查（适用等级：三级及以上）；

c) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备（适用等级：一级及以上）；

d) 应定期开展针对各岗位人员的数据安全相关的安全知识和技能培训，并进行考核（适用等级：

一级及以上）；

e) 应定期开展针对各岗位人员的数据安全相关管理规范、流程、制度培训，并进行考核（适用等级：二级及以上）；

f) 应加强对外部单位技术人员和外协人员的安全管理，访问受控区域前应先提出书面申请，批准后由专人全程陪同，并登记备案，必要时应签署保密协议，不得进行非授权操作，不得泄露、篡改、丢失和滥用数据（适用等级：二级及以上）。

5.3.4 安全审核

处理政务数据的信息系统安全审核应满足以下安全要求：

a) 应建立数据安全审核制度，明确数据安全审核的目的、内容和流程。应明确并建立对数据安全策略、访问控制变更、数据分级变更、通道安全配置、密码算法配置、密钥管理等保护措施的管理流程和审核机制（适用等级：一级及以上）；

b) 应明确并建立对数据共享、开放、使用、备份、存档、销毁等相关操作的安全管理流程和审核审批机制（适用等级：二级及以上）；

c) 应定期对接触个人信息、敏感数据和重要数据的人员进行安全审查、背景审查，对其操作日志进行分析，一旦发现违规行为，应根据严重程度采取相应的惩戒措施（适用等级：四级）；

d) 应对个人信息的重要操作（如进行批量修改、拷贝、下载等重要操作）进行安全审查，确保个人信息使用的安全性（适用等级：二级及以上）；

e) 应对数据导出操作进行安全审查，确保导出过程的规范性和安全性（适用等级：三级及以上）。

5.3.5 分级管理

处理政务数据的信息系统分级管理应满足以下安全要求：

a) 应以书面的形式说明数据的级别及确定级别的方法和理由（适用等级：一级及以上）；

b) 应保证定级结果经过相关部门的批准（适用等级：一级及以上）；

c) 应组织相关部门有关安全技术专家对数据分级结果的合理性和正确性进行论证和审定(适用等级：一级及以上）；

d) 应根据相关要求，将数据分级、数据共享/不共享、数据开放/不开放材料进行报备（适用等级：一级及以上）。

5.3.6 检查和考核

处理政务数据的信息系统检查和考核应满足以下安全要求：

a) 应定期进行常规安全检查，检查内容包括但不限于安全策略、账户管理、日志管理、平台日常运行、管理员日常操作、平台漏洞和数据备份等（适用等级：一级及以上）；

b) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报（适用等级：二级及以上）；

c) 应定期对数据安全管理各方面的内容进行全面安全检查，检查内容包括但不限于制度体系建设情况、安全策略执行情况、数据安全防护状况等内容（适用等级：三级及以上）。

5.3.7 安全评估

处理政务数据的信息系统安全评估应满足以下安全要求：

a) 应定期对信息系统安全状况和数据安全保护情况进行评估，发现安全问题及时整改，确保数据来源合法、质量可靠（适用等级：一级及以上）；

b) 应对数据的收集、存储、传输、处理、共享、开放、加工、使用、销毁等过程进行安全评估，

确保过程的规范性和安全性，防止个人信息、敏感数据和重要数据的泄露、篡改、丢失和滥用（适用等级：二级及以上）；

c) 应在数据级别发生变化时重新对新级别的数据安全保护情况进行评估，对不符合或不适用情况进行整改（适用等级：二级及以上）；

d) 涉及数据跨境传输的，应对其合规性和安全性进行评估，评估通过后才可进行相应操作（适用等级：二级及以上）；

e) 涉及在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，应符合国家网信部门会同国务院有关部门制定的办法和相关标准的要求（适用等级：三级及以上）；

f) 应在管理制度中明确数据的对外共享和开放，定期进行安全评估，及时发现和制止违规行为（适用等级：二级及以上）；

g) 应对多人操作行为进行安全评估，确保单人无法独立完成整个操作活动（适用等级：四级）；

h) 应对高风险操作可能对平台和数据造成的影响进行评估，评估通过后才可进行相应操作（适用等级：四级）。

5.3.8 应急处置

处理政务数据的信息系统应急处置应满足以下安全要求：

a) 应明确数据相关安全事件的上报和处置流程（适用等级：一级及以上）；

b) 应制定专门的应急预案，包括应急处理流程、系统恢复流程等内容，明确应急流程和人员分工，并定期开展应急演练（适用等级：二级及以上）；

c) 应采取技术措施实现实时安全预警，并及时处理发现的攻击事件或安全问题（适用等级：三级及以上）；

d) 应采用态势感知等相关技术，实现对平台或系统潜在安全风险尤其是高级持续性威胁（APT）等攻击行为的识别、分析和预警（适用等级：四级）。

5.3.9 安全监管

处理政务数据的信息系统安全监管应满足以下安全要求：

a) 应对数据安全相关的制度、策略、流程的落实情况进行监督，对发现的问题进行督促整改（适用等级：一级）；

b) 应建立数据安全监督管理机制，对本机构数据安全相关的制度、策略、流程的落实情况进行监督和管理，对发现的问题进行督促整改，对落实不力的情况进行惩戒（适用等级：二级及以上）；

c) 应积极接受并主动配合上级主管部门定期对本机构数据安全落实情况以及本机构数据安全保护情况进行监督和管理，并对发现的问题进行整改（适用等级：二级及以上）。

5.3.10 第三方服务商

处理政务数据的信息系统第三方服务商应满足以下安全要求：

a) 应确保第三方服务商的选择符合国家有关规定（适用等级：一级及以上）；

b) 应在服务协议中规定第三方服务商的责任与权限，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等（适用等级：一级及以上）；

c) 应在服务协议中规定服务合约到期时，完整提供所服务客户数据，并承诺相关数据进行清除（适用等级：一级及以上）；

d) 应与选定的第三方服务商签署保密协议，要求其不得泄露客户数据（适用等级：一级及以上）；

e) 应保证第三方服务商对客户系统和数据的操作可被客户审计（适用等级：一级及以上）。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[3] 《政务信息资源共享管理暂行办法》（2016年9月5日国务院〔2016〕51号文件印发）