ICS 

|  |
| --- |
|  |

DBXX

四川省地方标准

DB XX/ XXXXX—XXXX

|  |
| --- |
|  |

四川省政务数据 数据分类分级保护指南

(征求意见稿)

|  |
| --- |
|  |
|  |

XXXX - XX - XX发布

XXXX - XX - XX实施

四川省市场监督管理局   发布

目 录

[目 录 I](#_Toc9804)

[前 言 II](#_Toc21280)

[四川省政务数据 数据分类分级保护指南 3](#_Toc2681)

[1 范围 3](#_Toc14754)

[2 规范性引用文件 3](#_Toc16505)

[3 术语和定义 3](#_Toc29483)

[4 政务数据分类分级保护 3](#_Toc14563)

[4.1 原则 3](#_Toc29698)

[4.2 框架 4](#_Toc27840)

[4.3 分类要求 4](#_Toc22372)

[4.4 分级保护 4](#_Toc24398)

[4.4.1 保护级别 5](#_Toc23749)

[4.4.2 定级流程 5](#_Toc7853)

[4.4.3 保护措施 6](#_Toc31802)

[5 政务数据分类分级保护中的关键问题处理 6](#_Toc17207)

[5.1 基本遵循 6](#_Toc13057)

[5.2 问题处理 6](#_Toc10834)

[5.2.1 数据体量与保护级别的确定 6](#_Toc29060)

[5.2.2 数据聚合与数据保护级别的变更 6](#_Toc20721)

[5.2.3 数据时效性与数据保护级别的变更 7](#_Toc7759)

[5.3 持续优化 7](#_Toc4913)

[参 考 文 献 14](#_Toc32205)

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。

本文件由四川省大数据中心提出并归口。

本文件由四川省市场监督管理局批准。

本文件起草单位：×××

本文件主要起草人：×××

四川省政务数据 数据分类分级保护指南

1. 范围

本文件提出了四川省政务数据分类分级的原则、框架、保护措施和关键问题处置方法，规范了政务数据安全保护的基本技术与管理要求。

本文件适用于规范本地区政务部门（包括行政机关和具有公共事务管理职能的事业单位）在政务数据收集、存储、使用、加工、传输、提供、公开等生命周期的分类分级保护，也适用于监管部门对政务数据安全保护的监督，也适用于指导第三方机构的安全评估、合规检查等。

本文件适用于不涉及国家秘密信息的政务数据，核心数据、重要数据的界定和保护要求按照国家相关文件执行。

1. 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 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069-2022 信息安全技术 术语

GB/T 38664.1-2020 信息技术 大数据 政务数据开放共享 第1部分：总则

GB/T 40692-2021 政务信息系统定义和范围

DB51/T 3056-2023 政务数据 数据分类分级指南

DB51/T 3058-2023 政务数据 数据脱敏规范

1. 术语和定义

GB/T 25069-2022、GB/T 38664.1-2020、GB/T 40692-2021、DB51/T 3056-2023、DB51/T 3058-2023界定的以及下列术语和定义适用于本文件。

数据处理 data processing

包括政务数据的收集、存储、使用、加工、传输、提供、公开等。

[来源：中华人民共和国数据安全法]

1. 政务数据分类分级保护
   1. 原则

a）科学实用原则:从数据管理和使用方便的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需求对数据进行精细分类。

b）点面结合原则:数据保护定级既要考虑单项数据保护定级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据保护级别。

c）动态更新原则:根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级保护级别、重要数据目录等进行定期审核更新。

* 1. 框架

政务数据分类分级保护框架（见图1），对政务数据进行分类分级保护判定和实施，建立覆盖政务数据处理全过程的保护体系，明确组织架构、制度、人员、审计等方面，全面加强政府部门数据安全保护能力。主要内容包括政务数据分类要求和分级保护。

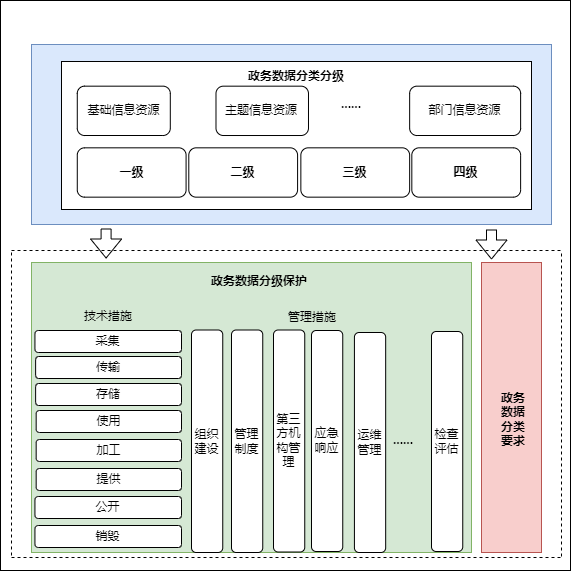


图1 政务数据分类分级保护框架

政务数据分类要求是按照政务数据具有的某种共同属性或特征（包括数据对象、重要程度、应用场景等），进行区分和归类。同时，根据数据所属领域相关法规、标准等进行保护。

政务数据分级保护包括技术措施和管理措施。技术措施是针对不同安全级别的数据，明确其在采集、传输、存储、处理、共享、公开以及销毁等各个环节的安全保护要求；管理措施从组织建设、管理制度、第三方管理以及检查评估等多个方面，规范人员行为，完善优化制度建设。

* 1. 分类要求

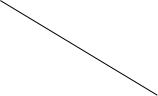
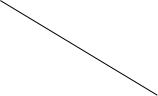
从数据管理、业务应用、安全保护、数据对象等不同维度，采用线、面以及综合等方法进行分类，遵循相应领域的法律法规、标准规范等要求实施，以便于管理和使用政务数据。

* 1. 分级保护

分级保护包括数据保护级别划分、定级流程和相应级别的保护措施。

* + 1. 保护级别

政务数据保护级别由高到低分为四级，分别为四级、三级、二级和一级，政务数据保护级别由信息系统网络安全保护等级和所承载数据级别综合得出，表1给出了政务数据保护级别判定方法。表1中政务信息系统安全保护等级执行GB/T 22240。

**表1 政务数据保护级别与政务数据级别、政务信息系统安全保护等级的关系**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据级别 政务 保护  信息系统 等级  安全保护等级 | 一级 | 二级 | 三级 | 四级 |
| 一级 | 一级 | \ | \ | \ |
| 二级 | 一级、二级 | 二级 | \ | \ |
| 三级及以上 | 一级、二级 | 二级、三级 | 三级 | 四级 |

* + 1. 定级流程

根据政务数据分级保护对象确定保护措施的一般流程，见图2。

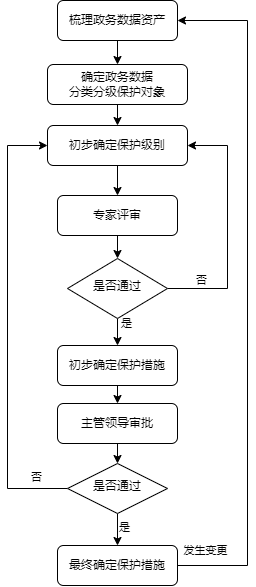


图2 政务数据保护级别定级流程

如图2 所示，政务数据分级保护的具体流程如下：

a)全面梳理政务数据资产。明确应用场景和数据责任主体，形成数据资产清单；

b)确定政务数据分级保护对象。初步确定拟分级保护的数据范围和对象；

c)初步确定数据保护级别。结合现有和可预期的数据应用场景，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、影响范围，参照表1初步确定数据保护级别（表1以结构化数据为例，分级实施）；

d)专家评审。组织网络安全和业务专家，对初步确定的数据安全保护级别进行评审，确保分级保护的准确性和科学性，若评审不通过，则应重新确定数据保护级别；

e)初步确定保护措施。根据数据保护级别，初步确定数据保护技术措施和管理措施；

f)主管领导审批。将通过专家评审的数据分级保护结果报主管领导审批；

g)确定保护措施。主管领导审批通过后，最终确定数据保护措施；

h)当发生以下情形时，应重新对数据进行分级：

1）政务数据保护对象发生了增加、减少、改变等情况影响数据级别的；

2）政务数据保护对象在汇聚、加工、分析等过程中级别发生变化或产生新数据（如脱敏后的数据、统计产生的数据等）；

3）政务数据应用场景发生变化导致数据保护级别变化。

* + 1. 保护措施

政务数据分级保护措施分为技术措施和管理措施两部分，具体参见附录A和附录B。

1. 政务数据分类分级保护中的关键问题处理

政务数据分类分级保护遵循明确的法律法规和标准指南，注重关键问题的处理和持续改进，确保政务数据的安全性和有效利用。

* 1. 基本遵循

a）政务数据要严格按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规来处理数据分类分级保护中的关键问题。

b）政务数据要参照国家标准《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）来评估和提升数据安全能力。

* 1. 问题处理

随着数据的受控共享、安全和隐私保护、处理性能等方面成为数据保护中的关键问题，要确定数据保护和利用之间的平衡点，为政务数据的保护和充分利用奠定基础。

* + 1. 数据体量与保护级别的确定

在进行数据保护定级时，根据行业机构规模、数据分类情况、影响范围和影响程度等多个因素，综合判定数据级别。对数据体量宜注意以下内容：

a）数据体量大，影响范围、影响程度宜从高考虑；

b）数据涉及访问量大或者共享规模大，影响程度宜从高考虑；

c）数据经汇聚后体量变大，依据5.2.2中指出的情形进行处理；

d）涉及个人信息的数据，不考虑数据体量大小，均从高定级，一般不低于本文件中确定的三级。

* + 1. 数据聚合与数据保护级别的变更

数据在生命周期中,因各类业务需要,可能需要将相同或不同保护级别的数据汇聚在一起进行分析、处理。对数据聚合的保护,宜注意以下内容:

a)因业务需要,将来自不同途径或不同系统的数据汇聚在一起,数据的原始用途或所在系统发生改变,需要对数据保护重新定级;

b)需要深入分析汇聚后数据是否可能较原始数据获得更多的信息,并判断汇聚后的数据安全属性(完整性、保密性、可用性)遭到破坏后的影响,以准确保护定级;

c)汇聚后数据保护级别一般不低于所汇聚的原始数据的最高保护级别。

* + 1. 数据时效性与数据保护级别的变更

数据在生命周期中,由于业务需要,可能在特定的时间,数据的保护级别需要调整,促进数据的公开、共享和应用。针对不同时间节点数据保护级别的界定,宜注意以下内容。

a)数据在确定保护级别之初即考虑数据的时效性,对数据保护级别进行评估,合理确定数据的保护级别；

b)将明显具有不同时效性的数据分不同的类别确定保护级别；

c)同一类数据,在某时间点前后具有不同的保护级别,宜清楚地说明时间点前后的保护级别,并说明时间点的触发条件。触发条件可以是某一具体时间,也可以是某一特定事项；

d)数据时效性要素、保护级别宜准确标识,并通知相关人员知悉。

* 1. 持续优化

政务数据保护应不断总结经验，改进和完善数据保护措施，提升政务数据管理的专业性和系统性。

附 录 A  
（规范性）  
政务数据保护技术措施

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 数据  处理  活动 | 保护措施 | 对应数据  保护级别 | | | |
| 一级 | 二级 | 三级 | 四级 |
| 政务数据收集安全 | 结合业务需求，采用口令、智能IC卡、生物特征等对数据收集的工具、系统、设备账号进行身份鉴别。 | ● | ● | ● | ● |
| 采用密码技术、双因素认证机制对数据收集的工具、系统、设备账号进行身份鉴别。 | 〇 | 〇 | ● | ● |
| 数据收集前，采用漏洞扫描、渗透扫描、压力测试等技术手段，对数据收集所使用的系统、设备、平台、接口以及软件等进行测试、安全评估。 | 〇 | 〇 | ● | ● |
| 在数据收集过程中采取安全协议、防火墙、WAF、入侵检测系统、数据泄露检测等技术措施防止数据泄漏。 | 〇 | ● | ● | ● |
| 采用加密技术、数据脱敏、访问控制等技术保障收集阶段数据机密性。 | 〇 | 〇 | ● | ● |
| 采用访问控制、API风险监测等技术手段，对数据采集API接口、网络访问接口等进行管理，降低数据泄露风险。 | 〇 | ● | ● | ● |
| 采用数据监测、数据审计等技术手段，实时监测数据收集行为，及时发现异常行为并发出告警。 | 〇 | ● | ● | ● |
| 采用行为匹配等技术措施，追踪、溯源数据泄露等风险行为，确保定位到人。 | 〇 | ● | ● | ● |
| 政务数据传输安全 | 根据实际情况，防火墙、WAF、安全网关、数据脱敏、数据校验、物理封装等措施保证数据传输安全。 | ● | ● | ● | ● |
| 采用安全传输通道、安全传输协议、抗DDoS等技术，保障数据传输过程中的机密性，提高数据传输可靠性和效率。 | 〇 | ● | ● | ● |
| 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机密性和完整性。 | 〇 | 〇 | ● | ● |
| 可采用单向隔离传输等技术手段，防范数据泄露。 | 〇 | 〇 | ● | ● |
| 采用数据监测、数据审计、全流量采集、态势感知和辅助决策等技术手段，实时监测数据传输异常，可对陌生IP地址、数据库异常连接等进行实时告警，在检测到数据遭破坏时能及时采取恢复措施。 | 〇 | 〇 | ● | ● |
| 采用网络攻击监测和防护，加密传输、完整性校验等技术手段保障数据导入导出过程中的安全，防止数据的可用性和完整性遭到破坏，降低可能存在的数据泄露等风险。 | 〇 | 〇 | ● | ● |
| 政务数据存储安全 | 根据实际情况，采用身份鉴别、访问控制、WAF等技术手段保障存储数据的安全访问，避免直接提供存储系统的公共信息网络访问。 | ● | ● | ● | ● |
| 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机密性和完整性。 | 〇 | 〇 | ● | ● |
| 采用数据冗余存储技术，增强数据存储的可靠性和稳定性。 | 〇 | 〇 | ● | ● |
| 采取安全检测工具，检测数据在存储过程中的异常行为，并实时告警。 | 〇 | 〇 | ● | ● |
| 采取数据库访问控制、数据库漏洞扫描、数据库运维管控等技术手段及时阻断、溯源异常数据访问、删除、修改等行为。 | 〇 | 〇 | ● | ● |
| 具备本地数据备份与恢复能力，备份介质场外存放。定期进行备份数据恢复演练。 | 〇 | ● | ● | ● |
| 具备异地备份能力，能够实现业务应用的快速恢复。 | 〇 | 〇 | ● | ● |
| 政务数据使用、加工安全 | 采用口令、智能IC卡、生物特征等技术手段对数据的使用加工进行验证；采用访问控制等技术手段进行授权。 | ● | ● | ● | ● |
| 采用数字签名等密码技术对数据的使用加工进行验证。 | 〇 | 〇 | ● | ● |
| 将数据使用加工中产生的过程数据与原始数据存储于不同的逻辑空间。 | 〇 | 〇 | ● | ● |
| 采用防火墙、WAF、主机安全、恶意代码检测、身份鉴别等技术手段，确保数据在使用加工中的环境安全。 | 〇 | ● | ● | ● |
| 在数据使用加工前，采用数据脱敏等技术，避免信息泄露。 | 〇 | ● | ● | ● |
| 在数据使用加工过程中，采用数据加密、完整性校验、安全审计、备份与恢复等技术手段，对数据进行保护，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。 | 〇 | ● | ● | ● |
| 远程加工、分析数据时，应严格限制数据加工、分析终端的外部接入IP数量和地址；不在数据加工、分析终端上保存数据。 | ● | ● | ● | 〇 |
| 采用数据异常监测、数据审计、数据安全态势感知等技术手段，及时发现、阻断和溯源数据异常使用加工行为。 | 〇 | 〇 | 〇 | ● |
| 政务数据提供（共享）安全 | 采取API接口全生命周期管理、访问控制等技术手段对数据共享接口进行管理，降低数据泄露风险。 | ● | ● | ● | 〇 |
| 采用白名单控制、监控进程等技术手段，对数据共享全链路各环节的权限最小化控制。 | 〇 | ● | ● | 〇 |
| 采用日志审计等技术，监控数据共享接口的调用信息、敏感内容等，分析是否存在恶意数据获取、异常数据外发等高风险行为。 | 〇 | ● | ● | 〇 |
| 结合数据共享场景、业务需要和安全风险评估结果，识别敏感数据或个人敏感信息，在数据共享前，对数据进行脱敏，避免信息泄露；非必要不提供原始数据。 | 〇 | ● | ● | 〇 |
| 采用数据加密等技术，避免信息泄露。 |  |  | ● | 〇 |
| 脱敏措施的部署应尽可能靠近数据源头，如数据库视图、应用系统底层API接口等。 | 〇 | 〇 | ● | 〇 |
| 特殊情况需要共享时，采用全流量采集、态势感知、接口数据监控和审计等技术手段，实时监测数据异常流量，及时进行问题跟踪溯源分析。 | 〇 | 〇 | 〇 | ● |
| 特殊情况需要共享时，采用数据治理平台等技术手段，管理数据血缘关系，包括数据加工、分析链路及映射关系等。 | 〇 | 〇 | 〇 | ● |
| 政务数据公开安全 | 采取安全协议、防火墙、WAF、安全网关、入侵检测系统等技术手段保障公开过程中的数据安全。 | ● | ● | ● | 〇 |
| 采取身份认证、访问控制、负载均衡等技术手段，管理数据公开所使用的接口，保证数据的机密性、完整性和可用性。 | ● | ● | ● | 〇 |
| 采用API风险监测、日志审计等技术，实时监控数据交换服务接口，监测数据异常外发等高风险行为，分析是否存在恶意数据获取、数据盗用等风险。 | 〇 | ● | ● | 〇 |
| 采取校验、数字签名、网页防篡改、网站黑链监测、网站挂码检测、网站可用性监测等技术措施对政务机构公开披露数据的真实性与完整性进行安全保护。 | ● | ● | ● | 〇 |
| 数据主管部门审批，有条件开放或无条件开放的,视情况采取数据脱敏、数据水印等技术手段，保证数据公开安全。 | 〇 | ● | ● | 〇 |
| 采用流量分析、日志审计、机器学习等技术手段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。 | 〇 | 〇 | ● | 〇 |
| 原则上不允许公开。 | 〇 | 〇 | 〇 | ● |
| 政务数据销毁安全 | 业务终止时采用删除、覆写法等方式销毁有关数据。 | 〇 | ● | ● | ● |
| 完全清除缓存中的数据，并在数据存储空间被释放或重新分配前完全清除数据，防止数据被恶意恢复。 | 〇 | 〇 | ● | ● |
| 物理销毁存储介质，保证在数据完全删除后再销毁存储介质，原则上不得以任何理由、任何方式对销毁数据进行恢复。 | 〇 | 〇 | 〇 | ● |

备注：“●”代表要求项需要参照执行，“〇”代表不需要考虑此项要求。

附 录 B  
（规范性）  
政务数据保护管理措施

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 管理措施 | 具体措施 | 对应数据  保护级别 | | | |
| 一级 | 二级 | 三级 | 四级 |
| 组织机构和人员管理 | 设置组织层面的数据安全管理部门、岗位和人员，并明确职能职责。 | ● | ● | ● | ● |
| 针对数据安全人员背景和专业能力进行审查，制定培训计划并定期开展培训，签订协议和责任书，制定考核等管理制度，动态调整人员数据访问使用权限。 | 〇 | ● | ● | ● |
| 设置数据安全工作领导小组，本单位法定代表人或者主要负责人是数据安全第一责任人。 | 〇 | ● | ● | ● |
| 设置安全审计、合规稽核、风险管理等相关岗位和人员。 | 〇 | 〇 | ● | ● |
| 设置数据销毁相关监督人员，对销毁过程进行监督等。 | 〇 | 〇 | ● | ● |
| 设置专职数据安全员。 | 〇 | 〇 | 〇 | ● |
| 管理制度 | 制定数据安全管理制度和业务相关的数据安全策略和规程，包括安全评估、安全审计、应急管理、审批审核等，并及时进行修订。 | ● | ● | ● | ● |
| 制定数据安全实施细则并定期修订。 | 〇 | ● | ● | ● |
| 识别并维护本机构数据资产清单，开展数据分类分级保护。 | ● | ● | ● | ● |
| 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，依据变更审批流程执行变更。 | 〇 | ● | ● | ● |
| 根据有关法规和制度要求，建立合理的密码使用和密钥管理技术规范和制度。 | 〇 | ● | ● | ● |
| 涉及数据跨境传输的情况，按照国家数据出境管理要求予以报备和评估。 | ● | ● | ● | ● |
| 依据国家有关规定与行业主管部门规章，在政务机构官方渠道披露数据，并在数据公开披露前，对拟披露数据审核与审批。 | ● | ● | ● | ● |
| 建立数据共享开放管理机制，签订数据安全承诺书、协议等，监督双方履行数据安全保护义务。 | 〇 | ● | ● | ● |
| 第三方机构管理 | 对参加数据处理活的第三方机构进行管理，针对具体业务场景签订安全协议、承诺书等，明确数据活动范围与权限，明确保密、安全等责任和义务。 | ● | ● | ● | ● |
| 与第三方机构解除合作关系时，要求第三方机构不再以任何方式保存合作期间所获取的数据及相关衍生数据，国家及行业主管部门另有规定的除外；若涉及向用户直接提供服务的第三方产品或服务，在与第三方机构解除合作关系时，明确告知用户已解除与第三方机构合作关系。 | ● | ● | ● | ● |
| 建立第三方机构审查与评估机制，定期评估其数据安全保护能力是否达到国家相应要求。 | 〇 | 〇 | ● | ● |
| 对第三方机构使用的工具或服务进行安全评估，验证自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的功能和安全性。 | 〇 | 〇 | ● | ● |
| 不可将存储三级及以上数据的数据库交由第三方机构运维。 | 〇 | 〇 | ● | ● |
| 应急响应 | 制定数据安全事件应急响应、处置上报流程。 | ● | ● | ● | ● |
| 制定数据安全事件应急预案，定期组织应急演练 | ● | ● | ● | ● |
| 实施数据安全事件处置的跟踪与过程管理，实现事件的闭环管理。 | 〇 | ● | ● | ● |
| 运维管理 | 按照业务需求、职责分离、安全保护策略及最小授权原则合理分配管理数据访问、处理权限，严格控制超级管理员权限账号数量。 | ● | ● | ● | ● |
| 授权特定人员进行数据批量复制、数据公开、数据销毁等数据处理活动的，由数据安全管理责任部门或者数据安全责任人审批。 | 〇 | 〇 | ● | 〇 |
| 针对个人信息、敏感数据、重要数据的访问等重要操作建立多方认证机制和审批机制，避免单个用户拥有过高的访问权限。 | 〇 | 〇 | 〇 | ● |
| 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，应建立统一、规范的采集流程，确保获得的同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。 | 〇 | ● | ● | ● |
| 第三方机构人员线下访问系统所在区域应执行严格的授权审批程序，使用明显标识标志其访客身份，全程人员陪同，记录出入时间，并限制和监控其活动范围。 | 〇 | ● | ● | ● |
| 建立数据泄露、数据篡改、数据窃取、数据非法使用的风险监控机制，主动预防、及时发现和终止数据泄露异常行为。 | 〇 | ● | ● | ● |
| 建立存放、使用、销毁等管理机制，对数据存储物理介质进行安全管控。 | 〇 | 〇 | ● | ● |
| 开展数据收集、存储、使用、加工以及销毁等处理活动前，明确涉及数据的用途、范围、数量、精度、频率、时段等具体规则。 | ● | ● | ● | ● |
| 对数据处理活动涉及的时间、范围、数据数量、数据类型、保护级别、频度、流向等详细信息进行记录。 | 〇 | ● | ● | ● |
| 定期开展行为审计。 | 〇 | 〇 | ● | ● |
| 对审计记录进行安全保护，防止未授权的访问和输出。 | 〇 | 〇 | 〇 | ● |
| 分权管理审计记录，针对不同的角色和组设置审计范围，保证审计数据的安全。 | 〇 | 〇 | 〇 | ● |
| 检查评估 | 每年开展一次数据安全相关自查和自评估，包括合规审查、安全巡检、安全评估等方面，及时整改风险问题。 | ● | ● | ● | ● |
| 委托第三方评估机构，每年至少开展一次数据安全相关检查评估，及时整改风险问题，并向主管部门报送检查评估报告。 | 〇 | ● | ● | ● |
| 在国家及主管部门的相关要求发生变化时，或在业务模式、业务功能、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，及时进行数据安全评估。 | 〇 | ● | ● | ● |
| 在新业务上线、数据迁移、数据出境、数据提供、委托处理等过程前，启动数据安全评估工作。 | 〇 | 〇 | ● | ● |
| 在数据开放、共享、使用、加工等处理活动前，对各数据内容、范围、时间周期、方式、安全管控手段要素进行数据安全风险评估。 | ● | ● | ● | ● |

备注：“●”代表要求项需要参照执行，“〇”代表不需要考虑此项要求。

参 考 文 献

1. 《中华人民共和国网络安全法》（2016年11月7日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[2] 《中华人民共和国数据安全法》（2021年6月10日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[3] 《中华人民共和国个人信息保护法》（2021年8月20日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[4] 《关键信息基础设施安全保护条例》（2021年4月27日国务院第133次常务会议通过）

[5] 《四川省数据条例》（2022年12月2日四川省第十三届人大常委会第三十八次会议审议通过）

[6] 《四川省“十四五”数字政府建设规划》

[7] 《四川省“十四五”新型基础设施建设规划》

[8] 《四川省省级政务信息化项目管理办法》（2021年10月5日发布）

[9] 《四川省网络安全事件应急预案（试行）》

[10] 《四川省省级部门政务信息资源接入省级共享平台指南（试行）》

[11] 《四川省政务信息资源共享平台资源申请、授权和使用管理细则（暂行）》

[12] 《国家政务服务平台安全保障要求》

[13] 《信息安全技术 数据安全能力成熟度模型》（GB/T 37988—2019 ）