ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

DB11

地 方 标 准

DB 11/T XXXXX—XXXX

政务数据分级与安全保护规范

Specificataion for government data classfication and security protection

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 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：北京市经济和信息化局、北京市大数据中心、北京信息安全测评中心、联通大数据有限公司、中电长城网际系统应用有限公司、北京金融大数据有限公司、北京科技大学、福建博思软件股份有限公司、中城智慧科技有限公司、北京知道创宇信息技术股份有限公司、北京观安信息技术有限公司、北京安华金和科技有限公司、北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司、北京明朝万达科技股份有限公司、九次方大数据信息集团。

本文件主要起草人：。

政务数据分级与安全保护规范

1 范围

本文件给出了政务数据分级的原则、方法、流程，规范了政务数据的安全保护通用要求、技术要求和管理要求，并给出了安全保护与共享开放之间的关系。

本文件适用于指导政务部门在政务数据采集、汇聚、传输、存储、加工、共享、开放、使用、销毁等全生命周期的分等级安全防护，也适用于指导网络安全主管部门对政务数据安全保护的监督管理。

本文件适用于不涉及国家秘密信息的政务数据。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息（在信息处理中） information（in information processing）

关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，在一定的场合中具有特定的意义。

[来源：GB/T 5271.1-2000,2.1]

3.2

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

[来源：GB/T 5271.1-2000,2.1]

3.3

政务数据 government 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、保存的结构化数据和非结构化数据，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的数据。

3.4

数据分级 data classification

对开放、共享和使用等过程中的政务数据，按照一定的原则和流程等方法将其划分为不同级别，以便对不同级别的数据实行有针对性的保护。

3.5

敏感数据 sensitive data

不为公众所知悉、具有价值并经权利人采取相应保密措施的数据。

3.6

个人信息 personal information

以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273-2020,3.1]

3.7

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[来源：GB/T 35273-2020,3.2]

3.8

重要数据 important data

组织的重要数字资产，一旦泄露或遭受破坏，极易导致组织遭受严重不良影响或毁灭性打击，严重危及个人生命和财产安全，损害社会公共利益甚至影响国家安全。

3.9

数据专区 data specific area

在特定的安全区域内、特定的监管条件下，对特定数据进行开放，引入社会力量开展数据汇聚融合、清洗加工、挖掘分析、产品服务等活动，推动大数据技术创新、应用创新、服务创新的支撑载体。

3.10

数据共享 Data sharing

政务部门因履行职责需要使用其他政务部门的政务数据或者为其他政务部门提供政务数据的行为。

3.11

数据开放 Data opening

政务部门面向公民、法人和其他组织提供政务数据的行为。

4 缩略语

下列缩略语适用于本文件。

IP 网络之间互联的协议（Internet Protocol）

APP 应用程序（Application）

APT 高级持续性威胁（Advanced Persistent Threat）

5 数据分级

5.1 分级原则

5.1.1 分级管控原则

分级防护，促进应用。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。

5.1.2 自主定级原则

自主分级，参考判例。政务部门应按照本文件的分级方法自主对数据进行分级，当已有相类似的数据分级案例时，应参考相似案例进行分级。

5.1.3 综合判定原则

场景导向，兼顾内容。数据分级时应结合数据的应用场景、组合、取值、数据量的大小等，力求数据分级准确合理。

5.2 分级方法

5.2.1 分级对象

5.2.1.1 从数据分级的粒度上分，可以对数据项进行分级，也可以对数据项集合进行整体分级，还可以既对数据项集合整体进行分级，又同时对其中的数据项进行分级。

5.2.1.2 当仅对数据项进行分级时，默认数据项集合的级别为其所包含数据项级别的最高级别。

5.2.1.3 当仅对数据项集合进行分级时，默认其包含的数据项级别为该数据项集合的级别。

5.2.1.4 当对数据项集合和其中的数据项同时分级时，数据项集合整体级别不应低于其包含数据项级别的最高级。

注：数据项既可以是单个非结构化数据，也可以是结构化数据中的单个数据字段。

5.2.2 分级因素

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、影响程度和影响范围。

5.2.3 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：

a）党政机关，指党的机关、人大机关、行政机关、政协机关、审判机关、检察机关、以及各级党政机关派出机构、直属事业单位及人民团体等。

b）公共服务机构，指教育、医疗、供水、供电、供气、供热、环保、公共交通、通讯等与人民群

众利益密切相关的公共企事业单位。

c）其他机构，指除党政机关、公共服务机构以外的企业和社会组织。

d）自然人，指依自然规律出生而取得民事主体资格的人。

5.2.4 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，见表 2。

表 1 影响程度

程度	定义
一般影响	数据发生泄露、篡改、丢失或滥用后对党政机关、公共服务机构、其他机构及自然人的运行、资产、安全造成轻微损害或一般损害，且结果可以补救。例如：对机构的相关工作产生轻微干扰，但工作仍可正常运转；对自然人造成轻微人身伤害或轻微财产损失。
严重影响	数据发生泄露、篡改、丢失或滥用后对党政机关、公共服务机构、其他机构及自然人的运行、资产、安全造成严重损害，且结果不可逆但可以采取措施降低损失。例如：对机构的相关工作产生较大干扰，但工作仍可继续运转；对自然人造成严重人身伤害或较大财产损失。
特别严重影响	数据发生泄露、篡改、丢失或滥用后对党政机关、公共服务机构、其他机构及自然人的运行、资产、安全造成特别严重损害，且结果不可逆。例如：对机构的相关工作产生极大干扰，导致工作运转失灵或几近瘫痪；致使自然人死亡或导致重大财产损失。

5.2.5 影响范围

数据发生泄露、篡改、丢失或滥用后的影响范围，根据其影响规模可划分为：较大范围影响和较小范围影响，根据其可控程度可划分为：强可控影响和弱可控影响，见表 3。

表 2 影响范围

影响范围		定义
影响规模	较小范围	数据发生泄露、篡改、丢失或滥用后，影响规模同时满足以下情形： a）影响党政机关、公共服务机构的数量，不超过 1 个。 b）影响其他机构的数量，不超过 3 个（含 3 个）。 c）影响自然人的数量，不超过 50 个（含 50 个）。
	较大范围	数据发生泄露、篡改、丢失或滥用后，影响规模满足以下情形之一： a）影响党政机关、公共服务机构的数量，超过 1 个。 b）影响其他机构的数量，超过 3 个。 c）影响自然人的数量，超过 50 个。
可控程度	强可控	数据发生泄露、篡改、丢失或滥用后，可控程度同时满足以下情形： a）可通过采取措施降低影响对象的数量或控制其增长。 b）影响仅发生在影响对象所在区域和行业，或可通过采取措施减少影响区域、行业数量，或缩小影响区域。 c）影响持续时间较短，或可通过采取措施缩减影响频次、周期，或能够在可知时间内消除影响。

影响范围		定义
	弱可控	数据发生泄露、篡改、丢失或滥用后，可控程度满足以下情形之一： a）影响对象的数量难以预知或难以控制。 b）影响涉及多个区域或跨行业，或影响区域、行业范围难以预知或难以控制。 c）影响持续时间较长，或影响频次、周期难以预知或难以控制，或难以在可知时间内消除影响。

5.2.6 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、影响范围，将数据划分为四级。具体描述，见表4。

表 3 分级定义

安全等级	数据发生泄露、篡改、丢失或滥用后的影响
一级	对党政机关、公共服务机构、其他机构、自然人造成较小范围且强可控的一般影响。
	对其他机构、自然人造成较小范围且弱可控的一般影响。
	对其他机构造成较大范围且强可控的一般影响。
二级	对党政机关、公共服务机构造成较小范围且弱可控的一般影响。
	对党政机关、公共服务机构、自然人造成较大范围且强可控的一般影响。
	对其他机构、自然人造成较大范围且弱可控的一般影响。
	对其他机构、自然人造成较小范围且强可控的严重影响。
三级	对党政机关、公共服务机构造成较大范围且弱可控的一般影响。
	对党政机关、公共服务机构造成较小范围且强可控的严重影响。
	对党政机关、公共服务机构、其他机构、自然人造成较小范围且弱可控的严重影响。
	对党政机关、公共服务机构、其他机构、自然人造成较大范围且强可控的严重影响。
	对其他机构、自然人造成较大范围且弱可控的严重影响。
	对其他机构造成较小范围且强可控的特别严重影响。
四级	对党政机关、公共服务机构造成较大范围且弱可控的严重影响。
	对党政机关、公共服务机构、自然人造成特别严重影响。
	对其他机构造成较小范围且弱可控的特别严重影响。
	对其他机构造成较大范围的特别严重影响。

5.2.7 分级因素与安全级别的关系

5.2.7.1 数据发生泄露、篡改、丢失或滥用后的影响对象、影响程度、影响范围等分级因素与安全级别对应关系，见表 5。

表 4 分级因素与安全级别的关系

影响程度	影响范围		影响对象		
	影响规模	可控程度	党政机关、公共服务机构	自然人	其他机构
一般影响	较小范围	强可控	一级	一级	一级
		弱可控	二级	一级	一级
	较大范围	强可控	二级	二级	一级

		弱可控	三级	二级	二级
严重影响	较小范围	强可控	三级	二级	二级
		弱可控	三级	三级	三级
	较大范围	强可控	三级	三级	三级
		弱可控	四级	三级	三级
特别严重影响	较小范围	强可控	四级	四级	三级
		弱可控	四级	四级	四级
	较大范围	-	四级	四级	四级

5.2.7.2　分级对象的影响对象涉及党政机关、公共服务机构、其他机构、自然人中的两类及两类以上时，分级对象级别应为其影响对象类别中的最高级。

5.2.7.3　由于数据项或数据项集合与业务应用场景有关，因此在不同应用场景下，数据的级别也会发生变化。本文件分别给出了不考虑应用场景和考虑应用场景下的部分数据项或数据项集合的分级示例，其中不考虑应用场景下的个人信息数据项分级示例见附录 A,不考虑应用场景下的运营商数据项分级示例见附录 B,某智慧停车应用场景下的数据项、数据项集合分级示例见附录 C,疫情防控应用场景下的数据项集合分级见附录 D。

5.3　分级流程

数据分级流程如图 1 所示，数据分级流程应符合下列规定：

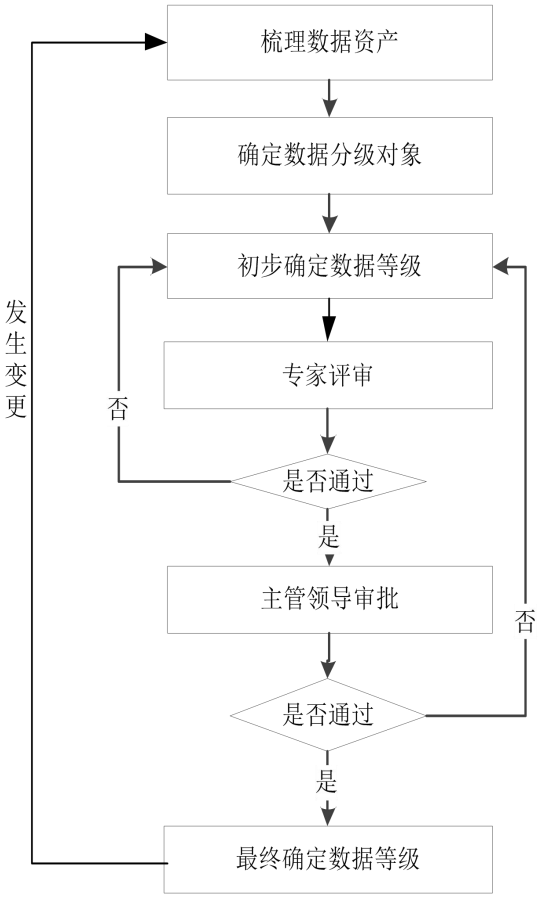

图 1　数据分级流程

a）梳理数据资产，形成数据目录是指全面梳理所拥有的数据资产，并形成数据目录。

1） 确定数据分级对象是指初步确定拟分级的数据范围和对象。

2） 初步确定数据等级是指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 4 初步确定数据等级。（以结构化数据为例，分级实施与级别判定流程示例，见附录 E）

3） 专家评审是指组织信息安全和业务专家，对数据初步分级结果进行评审，确保分级的准确性和科学性，若专家评审不通过，则应重新确定数据等级；

4） 主管领导审批是指将通过专家评审的数据分级结果报主管领导审批；

5） 最终确定数据等级是指主管领导审批通过后，最终确定数据等级；

6） 数据等级变更是指当应用场景、分级对象、数据级别等方面发生变化，导致数据发生泄露、篡改、丢失或滥用后的影响对象、影响程度、影响范围发生较大变化时，应按照本文件重新对数据进行分级。

b）数据分级发生变化的情形包括但不限于：

1） 数据分级对象发生了增加、减少、改变等情况；

2）数据在汇聚、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）数据应用场景发生变化导致数据级别变化。

6 数据分级安全保护要求

6.1 总体要求

6.1.1 数据安全保护应遵循政务部门负责、行业部门指导和监管的原则，落实数据保护的主体责任和监管职责。

6.1.2 数据安全保护应遵循国家网络安全等级保护、大数据安全相关法律法规及标准规范要求。

6.1.3 数据安全保护应依据本文件，根据数据级别采取相应的管理措施和技术手段对数据采集、汇聚、传输、存储、加工、共享、开放、使用、销毁等环节进行有针对性的保护，个人信息、敏感数据和重要数据要加强安全管控措施。

6.2 数据共享开放要求

6.2.1 对于各级数据的共享开放要求，见表5。

表 5 各级数据共享开放要求

数据等级	共享要求	开放要求
一级	无条件共享 （原则上无条件共享，如列为有条件共享，应当有法律、行政法规的规定或者相关政策为依据。）	无条件开放 （原则上在不违反法律法规的条件下，面向社会完全开放或脱敏后开放。）
二级	有条件共享 （原则上有条件共享，如列为不予共享，应当有法律、行政法规的规定或者相关政策为依据。）	有条件开放 （原则上在不违反法律法规的条件下，面向社会脱敏后有条件开放。）
三级		
四级	不予共享/有条件共享	不予开放/有条件开放

	（原则上不予共享，或提供可用不可见的有条件共享。）	（原则上不予开放，或在不违反法律法规的条件下提供可用不可见的有条件开放。）
注：可用不可见是指数据使用方不可以明细方式获取或访问数据，可以通过部署模型并通过数据建模分析获得或访问统计级结果数据以及模型自身参数。		

6.2.2 数据共享开放形态和分级管控要求应符合附录F的规定。

6.3 数据安全保护具体要求

6.3.1 数据安全保护要求分为通用要求、技术要求和管理要求三部分，其中通用要求规定了概括性、整体性的数据安全保护要求，技术要求规定了数据全生命周期的安全保护技术要求，管理要求规定了数据安全相关的组织机构、人员以及活动的安全保护管理要求。

6.3.2 各部分具体要求应符合附录G的规定。

附 录 A
（资料性）
不考虑应用场景下的个人信息数据项分级示例

A.1 概述

个人信息是政务数据的重要组成部分，个人业务应用在各类政务部门均有涉及，实际分级时要紧密结合个人信息的应用场景、个人信息数据项的组合、数据量的大小等，力求数据分级准确合理。

A.2 分级示例

在不考虑应用场景和较小范围影响规模的情况下，表A.2给出了一些典型个人信息单个数据项的分级示例。

表 A.2 典型个人信息分级示例参考

分类	数据项	影响对象	影响程度	影响规模	可控程度	安全等级
个人基本信息	姓名	自然人	一般影响	较小范围	强可控	一级
	生日	自然人	一般影响	较小范围	强可控	一级
	性别	自然人	一般影响	较小范围	强可控	一级
	民族	自然人	一般影响	较小范围	强可控	一级
	国籍	自然人	一般影响	较小范围	强可控	一级
	家庭关系	自然人	一般影响	较小范围	强可控	一级
	住址	自然人	一般影响	较小范围	强可控	一级
	个人电话号码	自然人	一般影响	较小范围	强可控	一级
	电子邮箱地址	自然人	一般影响	较小范围	强可控	一级
个人身份信息	身份证号码	自然人	严重影响	较小范围	强可控	二级
个人生物识别信息	基因	自然人	特别严重影响	较小范围	弱可控	四级
	指纹	自然人	特别严重影响	较小范围	弱可控	四级
	面部识别特征	自然人	特别严重影响	较小范围	弱可控	四级
网络标识信息	个人信息主体账号	自然人	严重影响	较小范围	强可控	二级
	IP 地址	自然人	严重影响	较小范围	强可控	二级
	个人数字证书	自然人	严重影响	较小范围	强可控	二级
个人医疗信息	病症	自然人	严重影响	较小范围	强可控	二级
	医嘱单	自然人	严重影响	较小范围	强可控	二级
	检验报告	自然人	严重影响	较小范围	强可控	二级
	手术及麻醉记录	自然人	严重影响	较小范围	强可控	二级
	用药记录	自然人	严重影响	较小范围	强可控	二级
	药物食物过敏信息	自然人	严重影响	较小范围	强可控	二级
	生育信息	自然人	严重影响	较小范围	强可控	二级
	以往病史	自然人	严重影响	较小范围	强可控	二级

分类	数据项	影响对象	影响程度	影响规模	可控程度	安全等级
	家族病史	自然人	严重影响	较小范围	强可控	二级
个人身体健康	体重	自然人	一般影响	较小范围	强可控	一级
	身高	自然人	一般影响	较小范围	强可控	一级
	肺活量	自然人	一般影响	较小范围	强可控	一级
个人工作信息	职业	自然人	一般影响	较小范围	强可控	一级
	职位	自然人	一般影响	较小范围	强可控	一级
	工作单位	自然人	一般影响	较小范围	强可控	一级
	工作经历	自然人	一般影响	较小范围	强可控	一级
个人教育信息	学历	自然人	一般影响	较小范围	强可控	一级
	教育经历	自然人	一般影响	较小范围	强可控	一级
	培训记录	自然人	一般影响	较小范围	强可控	一级
	成绩单	自然人	一般影响	较小范围	强可控	一级
个人财产信息	银行账户	自然人	严重影响	较小范围	强可控	二级
	鉴别信息(口令)	自然人	特别严重影响	较小范围	强可控	四级
	存款信息（包括资金数量、支付收款记录等）	自然人	严重影响	较小范围	强可控	二级
	房产信息	自然人	严重影响	较小范围	强可控	二级
	信贷记录	自然人	严重影响	较小范围	强可控	二级
	征信信息	自然人	严重影响	较小范围	强可控	二级
	交易和消费记录	自然人	严重影响	较小范围	强可控	二级
	流水记录	自然人	严重影响	较小范围	强可控	二级
	虚拟货币	自然人	严重影响	较小范围	强可控	二级
	虚拟交易	自然人	严重影响	较小范围	强可控	二级
	游戏类兑换码	自然人	一般影响	较小范围	强可控	一级
个人上网记录	网站浏览记录	自然人	一般影响	较小范围	强可控	一级
	软件使用记录	自然人	一般影响	较小范围	强可控	一级
	点击记录	自然人	一般影响	较小范围	强可控	一级
	收藏列表	自然人	一般影响	较小范围	强可控	一级
个人常用设备信息	硬件序列号	自然人	一般影响	较小范围	强可控	一级
	设备 MAC 地址	自然人	严重影响	较小范围	强可控	二级
	软件列表	自然人	一般影响	较小范围	强可控	一级
	唯一设备识别码	自然人	严重影响	较小范围	强可控	二级
个人位置信息	行踪轨迹	自然人	严重影响	较小范围	强可控	二级
	精准定位信息	自然人	严重影响	较小范围	强可控	二级
	住宿信息	自然人	严重影响	较小范围	强可控	二级
其他信息	婚史	自然人	一般影响	较小范围	强可控	一级
	宗教信仰	自然人	一般影响	较小范围	强可控	一级
	性取向	自然人	一般影响	较小范围	强可控	一级
	未公开的违法犯罪记录	自然人	严重影响	较小范围	强可控	二级

附 录 B
（资料性）
不考虑应用场景下的运营商数据项分级示例

B.1 运营商数据项分级示例

基于国内某通信运营商（以下简称：某运营商）的数据，依据本文件进行了分级示例，见表B.1。表中所列分级示例为不考虑应用场景的，结合运营商数据量在较大范围影响规模下的，单纯针对单个数据项的分级判定。实际分级时要紧密结合数据的应用场景、取值、数据量的大小等，力求数据分级准确合理。

表 B.1 某运营商数据分级示例参考

某运营商数据		本文件分级示例				
类别	对应字段	影响对象	影响程度	影响范围	可控程度	分级级别
位置数据-精准位置和行踪轨迹	装机地址	自然人	严重影响	较大范围	强可控	三级
	行踪轨迹	自然人	严重影响	较大范围	强可控	三级
	位置经纬度	自然人	严重影响	较大范围	强可控	三级
	小区代码	自然人	严重影响	较大范围	强可控	三级
	基站编号	自然人	严重影响	较大范围	强可控	三级
	位置文字描述	自然人	严重影响	较大范围	强可控	三级
通信详单	通话详单	自然人	严重影响	较大范围	强可控	三级
	短信详单	自然人	严重影响	较大范围	强可控	三级
	彩信详单	自然人	严重影响	较大范围	强可控	三级
	增值业务详单	自然人	严重影响	较大范围	强可控	三级
	上网流量详单	自然人	一般影响	较大范围	强可控	二级
部分用户画像	交往圈	自然人	一般影响	较大范围	强可控	二级
	家庭信息	自然人	一般影响	较大范围	强可控	二级
用户业务基本信息	用户状态	自然人	一般影响	较大范围	强可控	二级
	入网方式	自然人	一般影响	较大范围	强可控	二级
	入网起止时间	自然人	一般影响	较大范围	强可控	二级
	在网时长	自然人	一般影响	较大范围	强可控	二级
	停开机	自然人	一般影响	较大范围	强可控	二级
	协议起止时间	自然人	一般影响	较大范围	强可控	二级
	消费额度	自然人	一般影响	较大范围	强可控	二级
	发展渠道	自然人	一般影响	较大范围	强可控	二级
	发展人	自然人	一般影响	较大范围	强可控	二级
业务订购信息	业务订购	自然人	一般影响	较大范围	强可控	二级
合同信息	集团客户业务合同	其他机构	一般影响	较大范围	强可控	二级
	个人客户协议	自然人	一般影响	较大范围	强可控	二级
	优惠信息	自然人	一般影响	较大范围	强可控	二级

某运营商数据		本文件分级示例				
类别	对应字段	影响对象	影响程度	影响范围	可控程度	分级级别
围栏信息	是否在规定围栏范围内	自然人	严重影响	较大范围	强可控	三级
消费信息	预存款	自然人	严重影响	较大范围	强可控	三级
	缴费情况	自然人	严重影响	较大范围	强可控	三级
	付费方式	自然人	严重影响	较大范围	强可控	三级
	话费余额	自然人	严重影响	较大范围	强可控	三级
	受赠情况	自然人	严重影响	较大范围	强可控	三级
	交易历史记录	自然人	严重影响	较大范围	强可控	三级
账单	固定费用	自然人	严重影响	较大范围	强可控	三级
	通信费用	自然人	严重影响	较大范围	强可控	三级
	欠费信息	自然人	严重影响	较大范围	强可控	三级
客户服务信息	服务等级	自然人	一般影响	较大范围	强可控	二级
	信用等级	自然人	一般影响	较大范围	强可控	二级
	信用额度	自然人	一般影响	较大范围	强可控	二级
	积分	自然人	一般影响	较大范围	强可控	二级
	VIP 信息	自然人	一般影响	较大范围	强可控	二级
服务日志	Cookie 内容	自然人	一般影响	较大范围	强可控	二级
	上网日志	自然人	一般影响	较大范围	强可控	二级
	APP 使用日志	自然人	一般影响	较大范围	强可控	二级
	软件使用记录	自然人	一般影响	较大范围	强可控	二级
	点击记录	自然人	一般影响	较大范围	强可控	二级
部分用户画像	兴趣爱好	自然人	一般影响	较大范围	强可控	二级
	APP 偏好	自然人	一般影响	较大范围	强可控	二级
	终端偏好	自然人	一般影响	较大范围	强可控	二级
	内容偏好	自然人	一般影响	较大范围	强可控	二级
违规记录	垃圾短信记录	自然人	一般影响	较大范围	强可控	二级
	骚扰电话记录	自然人	一般影响	较大范围	强可控	二级
	诈骗电话记录	自然人	一般影响	较大范围	强可控	二级
	黑名单	自然人	一般影响	较大范围	强可控	二级

B.2 分级结果说明

本文件对某运营商数据的安全分级结果，与该运营商企业内现行数据安全等级的划分结果基本一致。其中，某运营商部分字段的分级结果偏高于本文件对该运营商数据的安全分级结果，是出于该运营商作为企业需加强对于用户相关信息与数据的保护，在本文件可接受范围，不影响本文件的兼容性、适用性。

附 录 C
（资料性）
某智慧停车应用场景下的数据项、数据项集合分级示例

基于国内某智慧停车项目的数据，依据本文件进行了分级示例，见表C.1。表中所列分级示例为结合停车场用户场景，在较大范围（用户量超过50人）的影响规模下的，针对单个数据项和数据项集合（包含多个数据项）的分级判定。实际分级时要紧密结合数据的应用场景、取值、数据量的大小等，力求数据分级准确合理。

表 C.1 某智慧停车项目数据分级示例参考

分类	数据项	影响对象	影响程度	影响规模	可控程度	安全等级
办证申请信息	申请用户姓名	自然人	一般影响	较大范围	强可控	二级
	电话	自然人	一般影响	较大范围	强可控	二级
	办证类型	自然人	一般影响	较大范围	强可控	二级
	小区名	自然人	严重影响	较大范围	强可控	三级
	楼号	自然人	严重影响	较大范围	强可控	三级
	家庭住址	自然人	严重影响	较大范围	强可控	三级
	车牌	自然人	严重影响	较大范围	强可控	三级
	旧车牌	自然人	严重影响	较大范围	强可控	三级
	车牌颜色	自然人	一般影响	较大范围	强可控	二级
	牌照类型	自然人	一般影响	较大范围	强可控	二级
	车主与户主关系	自然人	严重影响	较大范围	强可控	三级
	费用	自然人	一般影响	较大范围	强可控	二级
	操作员	自然人	一般影响	较大范围	强可控	二级
	身份证件编号	自然人	严重影响	较大范围	强可控	三级
	身份证姓名	自然人	严重影响	较大范围	强可控	三级
	房屋证明编号	自然人	严重影响	较大范围	强可控	三级
	房产证明姓名	自然人	严重影响	较大范围	强可控	三级
	户口本地址	自然人	严重影响	较大范围	强可控	三级
	户口本姓名	自然人	严重影响	较大范围	强可控	三级
	驾驶证编号	自然人	严重影响	较大范围	强可控	三级
	驾驶证姓名	自然人	严重影响	较大范围	强可控	三级
	行驶证编号	自然人	严重影响	较大范围	强可控	三级
	行驶证姓名	自然人	严重影响	较大范围	强可控	三级
	结婚证姓名	自然人	严重影响	较大范围	强可控	三级
	结婚证编号	自然人	严重影响	较大范围	强可控	三级
	租赁合同姓名	自然人	严重影响	较大范围	强可控	三级
	租赁合同编号	自然人	严重影响	较大范围	强可控	三级
	居委会	公共服务机构	一般影响	较大范围	强可控	二级
	办证申请信息数	自然人	特别严重影	较大范围	强可控	四级

分类	数据项	影响对象	影响程度	影响规模	可控程度	安全等级
	据项集合		响			
办证规则信息	车场名称	公共服务机构	一般影响	较大范围	强可控	二级
	免费时长	自然人	一般影响	较大范围	强可控	二级
	基础分钟数	自然人	一般影响	较大范围	强可控	二级
	基础分钟金额	自然人	一般影响	较大范围	强可控	二级
	累计金额	自然人	一般影响	较大范围	强可控	二级
	每日封顶	自然人	一般影响	较大范围	强可控	二级
	包月金额	自然人	一般影响	较大范围	强可控	二级
	更新时间	自然人	一般影响	较大范围	强可控	二级
	创建时间	自然人	一般影响	较大范围	强可控	二级
	操作员 id	自然人	一般影响	较大范围	强可控	二级
	证件类型	自然人	一般影响	较大范围	强可控	二级
	办证规则信息数据项集合	自然人	一般影响	较大范围	强可控	二级
停车场信息	车场编号	公共服务机构	一般影响	较大范围	强可控	二级
	车场名称	公共服务机构	一般影响	较大范围	强可控	二级
	居委会编号	公共服务机构	一般影响	较大范围	强可控	二级
	更新时间	自然人	一般影响	较大范围	强可控	二级
	创建时间	自然人	一般影响	较大范围	强可控	二级
	停车场信息数据项集合	公共服务机构	一般影响	较大范围	强可控	二级
站内通知信息	标题	自然人	一般影响	较大范围	强可控	二级
	类型	自然人	一般影响	较大范围	强可控	二级
	发布时间	自然人	一般影响	较大范围	强可控	二级
	内容	自然人	一般影响	较大范围	强可控	二级
	创建人	自然人	一般影响	较大范围	强可控	二级
	创建时间	自然人	一般影响	较大范围	强可控	二级
	修改人	自然人	一般影响	较大范围	强可控	二级
	修改时间	自然人	一般影响	较大范围	强可控	二级
	站内通知信息数据项集合	自然人	一般影响	较大范围	强可控	二级
公示登记信息	项目名称	自然人	一般影响	较大范围	强可控	二级
	公示图像文件	自然人	一般影响	较大范围	强可控	二级
	操作员编号	自然人	一般影响	较大范围	强可控	二级
	删除状态	自然人	一般影响	较大范围	强可控	二级
	更新时间	自然人	一般影响	较大范围	强可控	二级
	创建时间	自然人	一般影响	较大范围	强可控	二级
	公示状态	自然人	一般影响	较大范围	强可控	二级
公示登记信息	公示登记信息数据项集合	自然人	一般影响	较大范围	强可控	二级

附 录 D
（资料性）
疫情防控应用场景下的数据项集合分级示例

结合疫情防控所涉及的个人数据，依据本文件进行了分级示例，见表 D.1。表中所列分级示例为结合疫情防控应用场景的针对数据项集合的分级示例，在操作数据项集合的数据维度越多（列数越多）、操作数据项集合的数据量越大（行数越多）时，相应对影响程度、影响规模以及可控程度的判定范围越大、程度越深。

表 D.1 疫情防控数据分级示例参考

所操作数据项或数据项集合	数据量	影响对象	影响程度	影响规模	可控程度	安全等级
仅 1 列手机号或身份证号	1-50 行	自然人	一般影响	较小范围	强可控	一级
	50 行以上	自然人	一般影响	较大范围	弱可控	二级
姓名、身份证号、手机号中任 2 列	1-50 行	自然人	严重影响	较小范围	强可控	二级
	50 行以上	自然人	严重影响	较大范围	弱可控	三级
多字段数据（至少含姓名、身份证号、手机号、健康信息等数据项）	1-50 行	自然人	特别严重影响	较小范围	强可控	四级
	50 行以上	自然人	特别严重影响	较大范围	弱可控	四级

附 录 E
（资料性）
分级实施与级别判定流程示例

以结构化数据的数据项集合分级定级为例。数据安全等级划分以数据项集合（库表）为单位，结合数据项（字段）的含义和数据项集合的业务应用场景进行综合判定实施定级。分级判定流程包括数据项定级、数据项集合定级和最终定级三个步骤，见图 E.1。

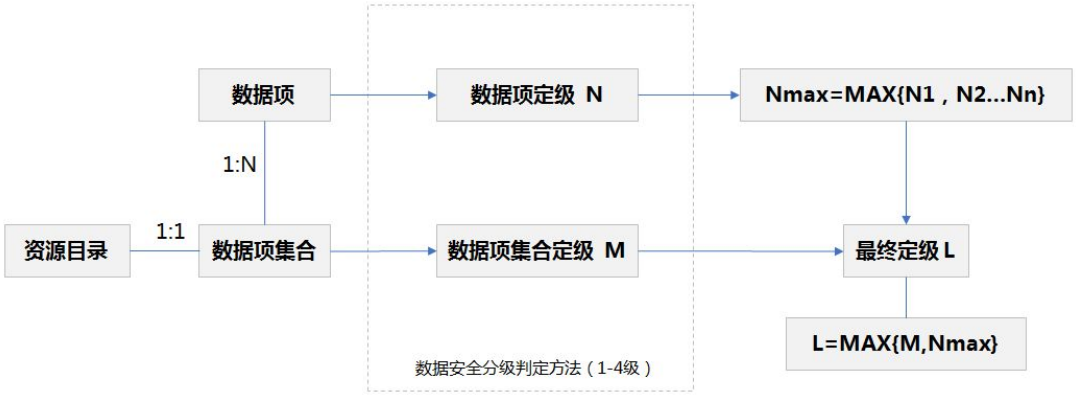

图 E.1 数据分级实施流程

各步骤解释说明如下：

a）数据项定级。依据数据项含义，对待定级数据项集合所包含的所有数据项，在不考虑应用场景前提下，进行等级划分，确定单个数据项的安全等级（N）；

b）数据项集合定级。依据数据项集合的业务应用场景以及与其它数据项集合的关联关系，对待定级数据项集合进行等级划分，确定数据项集合的安全等级（M）；

c）最终定级。步骤一的数据项定级最大值（$N_{max}=MAX\{N_1,N_2...N_n\}$）与步骤二的数据项集合定级（M），两者取最大值作为待定级数据项集合的最终定级（$L=MAX\{M,N_{max}\}$）。

附 录 F
（规范性）
数据共享开放形态分级管控

F.1 数据共享开放形态

数据共享开放过程中，依照数据加工和脱敏程度，对输出数据划分出原始数据、脱敏数据、统计数据三种形态，具体定义见表F.1。

表F.1 共享开放形态

可见程度	定义
原始数据	数据的原本形式和内容，未作任何加工处理。
脱敏数据	对各类重要数据、敏感数据所包含的敏感信息进行模糊化、加扰、加密或转换后（如：对身份证号码进行不可逆置换，但仍保持相应格式）形成的，无法通过推算演绎（含逆向推算、枚举推算等）、关联分析等方式识别出敏感信息的新数据。
统计数据	群体性综合性数据，是由多个个人或实体对象的数据进行统计或分析后形成的数据。如：群体位置轨迹统计信息、交易统计数据、统计分析报表、分析报告方案等。根据统计数据，应当无法推演、无法与其它数据关联间接分析出重要数据、敏感数据。统计数据中不应包括任何敏感信息。

F.2 数据共享形态分级管控

如表F.2所示，一级数据在共享时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在共享时，允许以原始数据、脱敏数据以及统计数据形态经加密处理后提供；四级数据在共享时，不允许以原始数据、脱敏数据形态提供，允许以统计数据形态经加密处理后提供。

表F.2 数据共享形态分级管控

安全等级	原始数据	脱敏数据	统计数据
一级	○	○	○
二级	○（加密）	○（加密）	○（加密）
三级	○（加密）	○（加密）	○（加密）
四级	×	×	○（加密）

F.3 数据开放形态分级管控

如表F.3所示，一级数据在开放时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在开放时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态经加密处理后提供；四级数据在开放时，不允许以原始数据、脱敏数据形态提供，允许以统计数据形态经加密处理后提供。

表F.3 数据开放形态分级管控

安全等级	原始数据	脱敏数据	统计数据

安全等级	原始数据	脱敏数据	统计数据
一级	○	○	○
二级	×	○（加密）	○（加密）
三级	×	○（加密）	○（加密）
四级	×	×	○（加密）

F.4　部门内数据加工、分析形态分级管控

如表 F.4 所示，一级数据在部门内加工、分析时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在部门内加工、分析时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态提供；四级数据在部门内加工、分析时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态经加密处理后提供。

表 F.4　部门内数据加工、分析形态分级管控

安全等级	原始数据	脱敏数据	统计数据
一级	○	○	○
二级	×	○	○
三级	×	○	○
四级	×	○（加密）	○（加密）

附 录 G
（规范性）
政务数据分级安全保护要求

G.1 通用要求

第一级至第四级数据的安全保护通用要求，见表G.1。

表 G.1 政务数据分级安全保护通用要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
A 通用要求	A1 系统安全	a1)承载本级数据的信息系统的安全保护应不低于等级保护一级的要求。	○			
		a2)承载本级数据的信息系统的安全保护应不低于等级保护二级的要求。		○		
		a3)承载本级数据的信息系统的安全保护应不低于等级保护三级的要求。			○	○
	A2 身份认证	a1)对登录信息系统的用户，应采用 “口令认证”等认证方式，进行身份鉴别；对线下访问操作数据的人员，应核验其身份信息。	○			
		a2)对登录信息系统的用户，应采用 “口令认证”和“动态口令”、“口令认证”和“数字证书认证”、“口令认证”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；对线下访问操作数据的人员，应核验其身份及其证件信息并进行登记。		○		
		a3)对登录信息系统的用户，应采用 “口令认证”和“数字证书实名认证”、“口令认证”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；对线下访问操作数据的人员，应核验其身份及证件信息，对证件信息进行复印件留存和登记。			○	○
		b)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。		○	○	○
		c)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，避免单个用户拥有过高的访问权限。			○	○
	A3 授权控制	a1)应建立基于主体角色的授权机制。	○			
		a2)应建立基于主体角色的授权机制，并在此基础上建立基于客体属性的授权机制。		○	○	○
		b)应建立统一的权限管理机制，实现系统用户的统一授权。		○	○	○
		c)应建立基于共享、开放任务的访问控制授权机制。		○	○	○
		d)应赋予操作主体最小操作权限和最小数据集。			○	○
		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。			○	○
		f)应建立统一数据出口授权管理机制，对数据共享、开放、使用等（包括但不限于：数据服务接口、数据文件等方式）进行统一授权审核管理、监控留痕和统一出口管控，依申请在对数据内容、提供形式、频率、周期等进行审核确认后，按共享或开放范围予以授权。			○	○
	A4 访问控制	a1)应建立基于主体角色授权的访问控制。	○			
		a2)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。		○	○	○
		b)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。		○	○	○
		c)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。			○	○
		d)应建立统一数据出口访问控制管理机制，对数据共享、开放、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			○	○

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
		请在对数据内容、提供形式、频率、周期等进行审核确认后，按共享或开放授权范围予以提供。				
A 通用要求	A5 数据标识	a)应标识数据的安全级别、共享属性、开放属性。	○	○	○	○
		b)应能在数据汇聚、存储、加工、共享、开放、使用等过程中识别数据的标识。		○	○	○
		c)应采取技术手段对数据资产进行管理。			○	○
	A6 安全审计	a)应对数据采集、汇聚、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。	○	○	○	○
		b)日志保存期限应不少于 6 个月。	○	○	○	○
		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。		○	○	○
		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。		○	○	○
		e)应建立对审计日志的大数据分析与事件挖掘机制，主动发现安全风险和隐患。				○
	A7 监测溯源	a1)应采取技术措施对数据采集、汇聚、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。	○			
		a2)应采取技术手段实时监控数据采集、汇聚、传输、存储、加工、共享、开放、使用等过程，及时发现和告警异常行为，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。		○	○	○
		b)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。	○	○	○	○
		c)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和数量，数据接收方等信息。		○	○	○
		d)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。			○	○
		e)应采取技术手段实现对数据专区内数据开放过程的实时监测，并记录和分析监测日志。			○	○
		f)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。		○	○	○
		g)应建立对数据血缘关系的管理和对数据加工、分析链路及映射关系的管理，记录加工、分析等处理环节的操作日志，包括但不限于：操作者、操作时间、操作对象、操作内容等。			○	○
注：“○”代表本要求项与该级数据存在对应关系。						

G.2 技术要求

第一级至第四级数据的安全保护技术要求，见表G.2。

表 G.2 政务数据分级安全保护技术要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
B 技术	B1 采集	a)应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性。	○	○	○	○
		b)应对数据采集终端、数据导入服务组件等的使用进行身份鉴别。	○	○	○	○
		c)应依据最小化原则实现采集账号认证及权限分配。		○	○	○

表 G.2　政务数据分级安全保护技术要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
要求	安全	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。		○	○	○
		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、具体的、清晰明确的意愿表示。		○	○	○
		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。		○	○	○
		g)利用信息系统、网站或 APP 采集个人信息时，应通过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、使用其个人信息的授权同意的方法。		○	○	○
		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。		○	○	○
	B2 汇聚安全	a)应对汇聚的数据进行完整性、一致性和真实性校验，避免数据遭受泄露、篡改、丢失。	○	○	○	○
		b)应根据数据的级别设置不同的级别标签。	○	○	○	○
		c)应能识别出个人信息、敏感数据和重要数据，并根据需要确定是否需要进行脱敏处理。		○	○	○
		d)应对个人信息设置特定标签。		○	○	○
		e)应采取技术手段和管理措施，防止数据汇聚过程中个人信息、敏感数据和重要数据的泄露、篡改、丢失。		○	○	○
		f)应采取技术措施对数据采集过程进行实时监控，及时发现和告警异常数据，并及时进行更正。			○	○
	B3 传输安全	a1)应采用校验技术保证通信过程中数据的完整性、一致性。	○	○		
		a2)应采用密码技术保证通信过程中数据的完整性、一致性。			○	○
		b1)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通信过程中的保密性。		○	○	
		b2)应采用国家密码管理部门核准的密码技术保证数据在通信过程中的保密性。				○
		c） 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。		○	○	○
	B4 存储安全	a)应提供数据的本地数据备份与恢复功能。	○	○	○	○
		b1)应设置数据存档规则，将暂时不使用的数据进行存档处理。	○	○	○	
		b2)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。				○
		c)应加强对存档设备的安全防护，防止敏感信息泄露。				○
		d)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。	○	○	○	○
		e)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。	○	○	○	○
		f1)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。		○	○	
		f2)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。				○
		g)应对不同安全等级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。		○	○	○
		h1)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。		○	○	
		h2)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。				○
		i)应设置个人信息的存储期限，确保存储期限为实现个人信息使用目的所必须的最短时间。		○	○	○
		j)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。			○	○
		k)个人生物识别信息应与其它信息分开存储。				○

表 G.2　政务数据分级安全保护技术要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
	B5 加工安全	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。	○	○	○	○
		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。	○	○	○	○
		c)应对加工、分析产生的新数据设置级别标签。	○	○	○	○
		d)外部远程加工、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。	○	○	○	
		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。				○
		f)内部远程加工、分析数据时，应严格限制数据加工、分析终端的数量和 IP 地址。	○	○	○	
		g)应不在数据加工、分析终端上保存数据。	○	○	○	○
		h1)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，确实需要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。		○	○	
		h2) 应能识别出个人信息、敏感数据和重要数据，并对其进行脱敏后再进行加工、分析。				○
		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。		○	○	○
		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。			○	○
	B6 共享安全	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。	○	○	○	○
		b1)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，确实需要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。		○	○	
		b2)只允许进行可用不可见的共享。				○
		c)应设置严格的访问控制策略，依据权限合理调配数据。		○	○	○
		d)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。		○	○	○
		e)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。				○
		f)应仅允许数据在本地导入、导出。			○	○
		g)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，并采取有效的保护个人信息主体的措施。	○	○	○	○
		h)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，严格限制对其进行的共享操作。				○
	B7 开放安全	a)应仅通过数据专区对外开放数据。	○	○	○	○
		b1)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。	○			
		b2)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。		○	○	○
		c)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。		○	○	○
		d)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。	○	○	○	○
		e1)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，确实需要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。		○	○	
		e2)只允许进行可用不可见的开放。				○
		f)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。		○	○	○
		g)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。				○

表 G.2　政务数据分级安全保护技术要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
		h)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。				○
		i)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。		○	○	○
		j)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。			○	○
	B8 使用安全	a)针对数据应用的访问，应进行应用认证和授权处理。	○	○	○	○
		b)应针对不同等级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。		○	○	○
		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，确实需要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。		○	○	○
		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。			○	○
		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。				○
	B9 销毁安全	a)应使用规范的工具或产品执行数据销毁工作。	○	○	○	○
		b)应确保以不可逆方式销毁数据及其副本内容。		○	○	○
		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。		○	○	○
		d1)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。			○	
		d2)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。				○

G.3　管理要求

第一级至第四级数据的安全保护管理要求，见表G.3。

表 G.3　政务数据分级安全保护管理要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
C 管理要求	C1 安全策略	a)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。	○	○	○	○
		b)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。	○	○	○	○
		c)应在数据分级的基础上，划分个人信息、敏感数据和重要数据范围，明确进行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。			○	○
	C2 安全机构	a)应设立数据安全管理的职能部门，设立数据管理员等负责人岗位，明确部门职能和岗位职责。	○	○	○	○
		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。		○	○	○
		c)应设立数据审计员、数据安全员等负责人岗位，明确部门职能和岗位职责。		○	○	○
		d)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。		○	○	○

表 G.3　政务数据分级安全保护管理要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
		e)应配备专职的数据安全员，不可兼任。				○
		f)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。				○
	C3 安全人员	a)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。	○	○	○	○
		b)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。		○	○	○
		c)应加强对外部单位技术人员和外协人员的安全管理，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。		○	○	○
	C4 安全审核	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、秘钥管理等保护措施的管理流程和审核机制。	○	○	○	○
		b)应明确并建立对数据汇聚、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机制。		○	○	○
		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。				○
		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。		○	○	○
		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。			○	○
	C5 分级和备案	a)应以书面的形式说明数据的安全级别及确定级别的方法和理由。	○	○	○	○
		b)应组织相关部门的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。	○	○	○	○
		c)应将数据分级备案材料报主管部门备案。	○	○	○	○
		d)应将数据共享、开放备案材料报主管部门备案。		○	○	○
		e)应将数据不共享、不开放备案材料报主管部门备案。				○
	C6 检查和考核	a)应定期进行常规安全检查，检查内容包括但不限于平台日常运行、管理员日常操作、平台漏洞和数据备份等。	○	○	○	○
		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。		○	○	○
		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。			○	○
		d)应将安全检查结果纳入部门年度考核范围。			○	○
	C7 安全评估	a)应对汇聚的数据进行安全评估，确保数据来源合法、质量可靠、不涉及国家秘密。	○	○	○	○
		b)应对数据的加工、分析、共享、开放、使用、备份、存档、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。		○	○	○
		c)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。	○	○	○	○
		d)应在信息系统发生重大变更时对当前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。			○	○
		e)应在数据级别发生变化时对当前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。		○	○	○
		f)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。		○	○	○
		g)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。			○	○
		h)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。		○	○	○

表 G.3　政务数据分级安全保护管理要求

管控类	管控域	安全要求项	保护要求			
			一级	二级	三级	四级
		i)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。				○
		j)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。				○
	C8 应急处置	a)应明确数据相关安全事件的上报和处置流程。	○	○	○	○
		b)应制定专门的应急预案，明确应急流程和人员分工，并定期开展应急演练。		○	○	○
		c)应制定个人信息安全事件应急预案,明确应急流程和人员分工,并定期开展应急演练。				○
		d)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。			○	○
		e)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 APT 等攻击行为的识别、分析和预警。				○
	C9 安全监管	a1)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。	○			
		a2)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。		○	○	○
		b)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。		○	○	○

参 考 文 献

[1] GB/T 5271.1-2000 信息技术词汇第1部分：基本术语

[2] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

[3] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[4] GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

[5] GB/T 35273-2020 信息安全技术 个人信息安全规范

[6] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

[7] GB/T 37973-2019 信息安全技术 大数据安全管理指南

[8] GB/T 39477-2020 信息安全技术型 政务信息共享 数据安全技术要求

[9] NIST SP 800-60 Vol.1 Rev.1 Guide for Mapping Types of Information and Information Systems to Security Categories