ICS 35.240
CCS Z 00

雄安新区地方标准

生态环境数据分级指南

Guidelines for ecological and environmental data classification

雄安新区生态环境监控中心　　发布

目 录

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。

本文件由雄安新区生态环境监控中心提出并归口。

1. 范围

本文件规定了生态环境数据分级原则、维度、要素、规则、流程、变更管理和分级管控措施。

本文件适用于雄安新区生态环境数据安全级别定级和管理工作。

本文件不适用于涉密数据分级管理。

2. 规范性引用文件

本文件内容引用了下列文件中的条款。凡是不注日期的引用文件，其有效版本适用于本文件。

GB/T 25069-2010 信息安全技术术语

GB/T 35295-2017 信息技术大数据术语

GB/T 38667-2020 信息技术大数据数据分类指南

GB/T 43697-2024 数据安全技术数据分类分级规则

DB36/T 1348—2020 生态文明数据分类及编码规范

3. 术语和定义

GB/T 25069-2010、GB/T 35295-2017、GB/T 38667-2020 和 GB/T 43697-2024 中确立的术语和定义，以及下列术语和定义适用于本文件。

3.1 数据分级 date grading

按照数据遭到破坏（包括攻击、泄露、篡改、非法使用等）后对国家安全、社会秩序、公共利益以及个人、法人和其他组织的合法权益（受侵害客体）的危害程度对公共数据进行定级，为数据全生命周期管理的安全策略制定提供支撑。

3.2 分类 classification

按照选定的属性（或特征）区分分类对象，将具有某种共同属性（或特征）的分类对象集合在一起的过程。

[DB36/T 1348—2020，术语和定义 3.2]

4. 数据分级对象

雄安新区生态环境局机关各科室、直属单位〔以下简称各科室（单位）〕在依法履职过程中获取和产生的各类数据（包括数据表、文件、图片、影像、视频

等数据）按照本标准进行分级管理。数据分级对象不包含涉及国家秘密的数据，涉及国家秘密的数据按照有关规定管理。

5. 数据分级原则

5.1 精准管控原则

参照生态环境信息资源目录规范，按照综合政务、综合业务、科技支撑、自然生态保、水生态环境、大气环境、噪声与振动、应对气候变化、土壤生态环境、固体废物与化学品、环评许可、环境监测、督察执法、宣传教育、环境应急、生态环境相关信息十六个一级类目对数据分类四级目录下的数据项进行分级，如四级目录为空，原则上应完善四级目录数据项后，再进行分级；如暂对三级目录数据项进行分级，该三级目录数据项下新增四级目录数据项后，原三级目录数据项数据分级失效，需重新对四级目录数据项进行分级。

5.2 就高从严原则

数据分级采用就高不就低原则，如四级目录数据项中包含多个级别数据内容的，该四级目录数据项按照所包含数据的最高级别进行定级。

5.3 动态调整原则

重要数据和核心数据实行动态管理。各科室（单位）经认定的重要数据和核心数据因重要性、精度、规模、安全风险等级等影响发生变化时，需在 15 个工作日内提出重要数据和核心数据调整申请。数据分级完成后，出现下列情形之一时，应进行数据级别变更：

a) 数据内容发生变化，导致原有数据的安全级别不再适用；

b) 数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生变化；

c) 多个原始数据直接合并，导致原有的安全级别不再适用合并后的数据；

d) 因对不同数据选取部分数据进行合并形成的新数据，导致原有数据的安全级别不再适用合并后的数据；

e) 不同数据类型经汇聚融合形成新的数据类别，导致原有的数据级别不再适用于汇聚融合后的数据；

f) 数据进行脱敏或删除关键字段，或者经过去标识化、假名化、匿名化处

理；

g) 发生数据安全事件，导致数据敏感性发生变化；

h) 因国家或行业主管部门要求，导致原定的数据级别不再适用；

i) 需要对数据安全级别进行变更的其他情形。

6. 数据分级维度

在数据分类的基础上，对数据目录下数据项的安全等级进行划分。按照影响对象、影响范围、影响程度（见附录 A），将雄安新区生态环境数据安全等级分为核心数据、重要数据、一般数据。各科室（单位）可根据业务需要，按照数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对社会稳定、公众利益或个人、组织合法权益造成的危害程度，对一般数据自行划定安全级别。一般数据依法流通，重要数据控制出境，核心数据使用和共享从严管控（见附录 B），未经新区网信安全部门批准，核心数据不得跨存储位置流动。

6.1 重要数据

重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露、篡改、破坏或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的数据，一般不作为重要数据，如生态环境领域碳排放、核与辐射、关键信息基础设施、公文、涉镉土壤污染数据等数据，重要数据包括但不限于：

（一）对国家安全、经济竞争实力有直接影响的科学技术成果数据；

（二）国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；

（三）达到国家有关部门规定的规模或者精度的国家基础数据；

（四）国家基础设施、关键信息基础设施建设运行及其安全数据；

（五）存储、处理个人信息数据量超过 100 万人的数据；

（六）经评估认定的其它数据。

6.2 核心数据

核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大以上规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。

主要包括：关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经评估确定的其他数据。

6.3 一般数据

除核心数据和重要数据以外的数据，一般数据可根据业务需要，划分为四级。

a) 1 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，不会对个人权益、组织合法利益造成危害，1 级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量及类别，避免由于类别较多或者数量过大被用于关联分析，在生态环境领域，属于公开开放数据。

b) 2 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织合法利益造成一般危害。2 级数据通常在组织内部、关联方共享和使用，相关方授权后可向组织外部共享，在生态环境领域，属于对内无条件共享数据。

c) 3 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织合法利益造成严重危害。3 级数据仅可由组织内部、关联方共享使用，相关方授权后可以向组织外部共享，在生态环境领域，属于对内有条件共享数据。

共享条件包括：

1）依申请共享：各部门提出申请，理由充分即可共享；

2）依政务事项共享：本部门开展政务事项需共享，且提供充分证明材料即可共享；

3）依法律法规要求共享：依据相关法律法规需共享，且提供相应法律法规条文即可共享；

4）其他特殊情况需要共享：办理其他业务且经相关批准后可共享。

d) 4 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织合法利益造成特别严重危害，或可能对公共利益、社会稳定造成一般危害。4 级数据按照批准的权限列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播，在生态环境领域，属于除严格审批不予共享数据。

7. 数据分级管理

数据分级是一项长期工作，各科室（单位）需按照本文件规定持续开展，科学、准确、完整识别本科室（单位）一般数据、重要数据和核心数据。对已有数据，由新区生态环境局网信领导小组办公室牵头、各科室（单位）配合，填报数据分级信息（见附录 C），对新建信息系统，在信息系统验收上线前，责任科室（单位）需上报数据分级信息，非信息系统获取和产生的数据，在数据获取和产生后的 15 个工作日内，按流程上报数据分级信息。

新区生态环境局网信领导小组统筹管理局本级数据分级工作，建立数据安全管理责任和评价考核制度。局网信领导小组办公室负责落实网信领导小组各项工作安排部署，组织各科室（单位）开展数据分类工作。各科室（单位）按照统一要求开展本科室（单位）数据安全管控和使用，并指定专人对本科室（单位）数据分类分级情况进行管理，按照“谁管业务、谁管业务数据、谁管数据安全”的原则，对本科室（单位）数据安全工作负主体责任，各科室（单位）党政主要负责人是第一责任人，数据使用或管理人员是直接责任人。局数据管理部门提供数据安全技术支撑，组织开展数据安全教育培训，并负责保障数据中心数据安全。

经雄安新区生态环境局综合组审核形成的雄安新区生态环境局本级数据分级情况，按规定程序和要求报送河北省网信办和河北省委国安办。

附录 A 数据安全级别影响因素

数据安全级别与影响对象、影响范围、影响程度的对应关系如表 A.1。

表 A.1 数据安全级别和分级因素关系矩阵

影响程度	影响范围	影响对象					
		国家安全	经济运行	社会稳定	公共利益	个人权益	组织权益
无影响	/	N/A	N/A	N/A	N/A	一般数据	一般数据
一般	较小	N/A	N/A	N/A	N/A	一般数据	一般数据
	较大	N/A	一般数据	一般数据	一般数据	一般数据	一般数据
	超大	重要数据	一般数据	一般数据	一般数据	一般数据	一般数据
严重	较小	N/A	N/A	N/A	N/A	一般数据	一般数据
	较大	N/A	重要数据	重要数据	重要数据	一般数据	一般数据
	超大	核心数据	重要数据	重要数据	重要数据	一般数据	一般数据
特别严重	较小	N/A	N/A	N/A	N/A	一般数据	一般数据
	较大	N/A	核心数据	核心数据	核心数据	一般数据	一般数据
	超大	核心数据	核心数据	核心数据	核心数据	一般数据	一般数据

A.1 影响对象

影响对象是指一旦数据遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象。影响对象通常包括国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益。

1.国家安全

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响国家政治、国土、经济、科技、文化、社会、生态、军事、网络、人工智能、核、生物、太空、深海、极地、海外利益等领域国家利益安全。

国家安全考虑因素（包括但不限于）：

a）影响国家政权安全、政治制度安全、意识形态安全、民族和宗教政策安全

b）影响领土安全、国家统一、边疆安全和国家海洋权益

c）影响基本经济制度安全、供给侧结构性改革、产业链和供应链安全、粮食安全、能源安全、重要资源安全、系统性金融风险、国际开放合作安全

d）影响我国科技实力、科技自主创新、关键核心技术、国家科技竞争力、科技伦理风险、出口管制物项

e）影响我国文化自信、社会主义核心价值观、文化软实力、中华优秀传统文化等

f）影响我国社会治理体系、社会治安防控体系、应急管理体系等

g）影响我国生态环境安全、绿色生态发展、污染防治、生态系统质量和稳定性、生态环境领域国家治理体系等

h）影响我国国防和军队现代化建设等，或者可被其他国家或组织利用发起对我国的军事打击

i）影响我国网络空间安全、关键信息基础设施安全、新一代人工智能安全，或者可能被利用实施对关键信息基础设施，核心技术设备等的网络攻击，可能导致特别重大或重大网络安全和数据安全事件

j）影响核材料、核设施、核活动情况，或可被利用造成核破坏或其他核安全事件

k）影响国家生物安全治理体系、生物资源和人类遗传资源安全、生命安全和生物安全领域的重大科技成果、疾病防控和公共卫生应急体系安全，或者可能导致重大传染病、重大生物安全风险

l）影响我国在太空、深海、极地等领域的国家利益和国际合作安全

m）影响我国企业海外投资、海外重大项目和人员机构安全、海外能源资源安全、海上战略通道安全，或可被利用实施对我国参与国家经贸、文化交流活动的破坏或对我国实施歧视性禁止、限制或其他类似措施

2、经济运行

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响市场经济运行秩序、宏观经济形势、国民经济命脉等经济利益。

经济运行考虑因素（包括但不限于）：

a）影响市场准入、市场行为、市场结构、商品销售、交换关系、生产经营秩序、涉外经济关系等市场经济运行秩序

b）影响社会总供给和总需求、国民经济总值和增长速度、国民经济中主要比例关系、物价总水平、劳动就业总水平与失业率、货币发行总规模与增长速度、进出口贸易总规模与变动等宏观经济形势

c）影响行业领域的生产、流通、分配、消费等经济活动，产业链、供应链或经济效益

d）影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业，

提供重要公共产品的行业、重大基础设施和重要矿产资源行业等国民经济命脉

3、社会稳定

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响社会治安和公共安全、社会日常生活秩序、民生福祉、法治和伦理道德等。

社会稳定考虑因素（包括但不限于）：

a）导致重大突发事件、群体性事件、社会矛盾激化、暴力恐怖活动、社会治安问题等

b）影响人民群众的民生保障或日常生活秩序，如扶贫、就业、收入、教育、文化体育、健康、养老和社保等民生事项或供电、供气、供水等基本服务保证工程

c）影响各级党政机关依法履行公共管理和服务职能

d）影响企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、卫生秩序

e）影响公共场所的活动秩序、公共交通秩序

4、公共利益

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响社会公众使用公共服务、公共设施、公共资源或影响公共健康安全等。

公共利益考虑因素（包括但不限于）：

a）影响对重大疾病尤其是传染病的预防、监控和治疗，或者可能引发突发公共卫生事件、造成社会工作健康危害

b）影响社会成员使用公共设施

c）影响社会成员获取公开数据资源

d）影响社会成员接受公共服务等方面

e）其他影响共利益、社会秩序等数据

5、组织权益

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响法人和其他组织的生产运营、声誉形象、公信力、知识产权等。

组织权益考虑因素（包括但不限于）：

a）可能导致组织遭到监管部门处罚、安全事件或法律诉讼

b）影响组织的重要或关键业务生产经营

c）造成组织经济损失

d）破坏组织声誉形象、公信力等

e）影响组织的知识产权、技术损失等

f）其他影响法人、非法人组织合法权益的数据

6、个人权益

数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能直接影响自然人的人身权、财产权以及其他合法权益。

个人权益考虑因素（包括但不限于）：

a）可能导致自然人的人格尊严收到侵害

b）影响自然人的人生安全

c）影响自然人的财产安全

d）其他影响个人权益的数据

A.2 影响程度

影响程度是指数据一旦泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可以分为特别严重危害、严重危害、一般危害。不同影响对象的影响程度描述见表 3。如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准。如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。

表 3 影响对象的影响程度描述

影响对象	影响程度	参考说明
国家安全	特别严重危害	直接影响国家政治安全
	严重危害	关系国家安全重点领域，或者对国土、经济、科技、文化、社会、生态、军事、网络、人工智能、核、生物、太空、深海、极地、海外利益等任一领域国家安全造成严重威胁
	一般危害	对国土、经济、科技、文化、社会、生态、军事、网络、人工智能、核、生物、太空、深海、极地、海外利益等任一领域国家安全造成直接威胁
经济运行	特别严重危害	1.直接影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业、提供重要公共产品的行业、重大基础设施和重要矿产资源行业等关系国民经济命脉行业的运行和发展 2.关系国民经济命脉，严重危害对社会经济发展具有重大影响的部门、企业、资源、区域等的生产运营和经济利益

		3.直接对多个行业领域，或者对行业领域核心业务、重要骨干企业、关键信息基础设施、重要资源等生产运营造成特别严重影响，例如导致大范围停工停产、大面积业务中断、大规模基础设施瘫痪、大量处理能力丧失等
	严重危害	1.直接影响宏观经济运行状况和发展趋势，如社会总供给和总需求、国民经济总值和增长速度、国民经济主要比例关系、物价总水平、劳动就业总水平与失业率、货币发型总规模、净出口贸易总规模与变动等 2.直接影响行业内多个企业、大规模用户，对行业发展、技术进步和产业生态等造成严重影响，或者直接影响行业领域核心竞争力、关键产业链、核心供应链等
	一般危害	1.对行业领域发展、生产、运行和经济效益等造成一般危害 2.直接危害市场运行秩序，如市场准入、市场行为、商品销售、交换关系、生产经营秩序等
社会稳定	特别严重危害	1.直接影响人民群众重要民生保障的事项、物资、工程或项目等 2.直接导致特别重大突发事件、特别重大群体性事件、暴力恐怖活动等，引起大范围社会恐慌，对社会稳定造成特别严重危害
	严重危害	1.直接导致重大突发事件、重大群体事件等，引起社会矛盾激化，对社会稳定造成严重危害 2.严重影响人民群众的日常生活秩序 3.严重影响各级党政机关履行公共管理和服务职能 4.严重影响法治和社会伦理道德规范
	一般危害	1.对人民群众的日常社会秩序造成一般影响 2.直接影响企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序 3.直接影响公共场所的活动秩序、公共交通秩序
公共利益	特别严重危害	1.关系重大公共利益，导致多个省市大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员无法使用公共设施，获取公开数据资源、接受公共服务 2.可能导致特别重大网络安全和数据安全事件，对公共利益造成特别严重影响，社会负面影响大 3.可能导致特别重大突发公共卫生事件，造成社会公众健康特别严重损害的重大传染病疫情，群体性不明原因疾病，重大食物和职业中毒等严重影响公众健康的事件
	严重危害	1.直接危害公众健康和安全，如严重影响迎请防控、传染病的预防监控和治疗等 2.可能导致重大突发公共卫生事件，造成社会公众健康严重损害的重大传染病疫情，群体性不明原因疾病，重大食物和职业中毒等严重影响公众健康的事件 3.导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员无法使用公共设施、获取公开数据资源、接受公共服务

	一般危害	对公共利益产生一般危害，影响较小范围社会成员使用公共设施，获取公开数据资源、接受公共服务
组织权益	特别严重危害	可能导致组织遭到监管部门严重处罚（包括取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产
	严重危害	可能导致组织遭到监管部门处罚（包括一段时间内暂停经营资格或业务等），或者影响部分业务无法正常开展的情况，造成较大经济或技术损失，破坏机构声誉
	一般危害	可能导致个别诉讼事件，或在某一时间造成部分业务中断，是组织的经济利益、声誉、技术等轻微受损
个人权益	特别严重危害	个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，容易导致自然人的人格尊严收到侵害或者人身、财产安全受到侵害，如遭受无法承担的债务、市区工作能力、导致长期的心理或生理疾病、导致死亡等
	严重危害	个人信息主体可能遭受较大影响，个人信息主体克服难度高、消除影响代价较大，如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等
	一般危害	个人信息主体可能会遭受困扰，但尚可以克服，如副处额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等

A.3 影响范围

根据数据发生泄漏、篡改、丢失或滥用后的影响规模大小，将影响范围分为较小范围、较大范围和超大范围。

其中涉及自然人的数量范围参照《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《网络安全审查办法》，具体描述见表 1：

表 1 数据影响范围描述

较小范围	数据发生泄漏、篡改、丢失或滥用后，影响的规模同时满足以下情形： a）不影响国家安全。 b）影响自然人不超过一定数量，其中： 1)敏感个人信息遭破坏影响不超过 50 人； 2)一般个人信息遭到破坏影响不超过 5000 人。
较大范围	数据发生泄漏、篡改、丢失或滥用后，影响的规模同时满足以下情形： a）影响的组织涉及公共利益，但不影响国家安全； b）影响自然人数量介于较小范围和超大范围之间。
超大范围	数据发生泄漏、篡改、丢失或滥用后，影响的规模同时满足以下情形： a）影响国家安全； b）影响自然人数量超过 100 万。

参照《个人信息保护法》《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《信息安全技术个人信息安全规范》（GB/T35273-2020），自然人个人信息，包括姓名、身份证号码、通信通讯联系方式、住址、账号密码、财产状况、通信记录、征信信息、住宿信息、交易信息、健康生理、行为轨迹等。自然人信息敏感程度见表 2：

表 2 个人信息敏感程度描述

敏感程度	信息类别	信息内容
敏感个人信息	特定身份	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证、港澳台通信证等
	生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
	身份鉴别信息	用于验证主体是否具有访问或者使用权限的信息，包括但不限于登录密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码、口令、动态口令、口令保护答案、短信验证码、密码提示问题答案、随机令牌等
	财产信息	征信信息、交易和消费信息、金融账户（包括但不限于支付账号、银行卡磁道数据或芯片等效信息、证券账户、基金账户、保险账户、其他财富账户、公积金账户、公积金联名卡账号、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
	行踪轨迹	基于实时地理位置形成的个人行踪和行程信息，例如实时定位信息、GPS 车辆轨迹信息、出入境记录、住宿信息（定位到街道、小区甚至更精确位置的数据）等
	医疗健康	个人因生病治疗等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史、健康生理信息
	其他敏感信息	宗教信仰、通讯记录和内容、性取向、婚史、未公开的违法犯罪记录、好友列表、群组列表、网页浏览记录、
	不满十四周岁未成年人的所有个人信息（包括敏感个人信息和一般个人信息）	
一般个人信息	除敏感个人信息以外的其他个人信息	

附录 B 数据分级管控措施

严格按照《网络安全法》《数据安全法》《个人信息保护法》《网络安全数据管理条例》等法律法规要求，制定数据分级管控措施，全面保证数据安全和合法合规使用。

B.1 核心数据

《网络数据安全管理条例（征求意见稿）》规定，国家对核心数据实行严格保护；处理核心数据的系统依照有关规定从严保护；数据处理者应当使用密码对重要数据和核心数据进行保护。

根据法律法规的相关要求，以及生态环境行业主管部门的有关规定，雄安新区生态环境局核心数据管控要求为：

未经河北省网信办和河北省国安办批准，核心数据不得跨主体流动。

核心数据的传输、存储均使用核心密码进行加密，无密码权限，任何人不能查看、处理和使用核心数据。

处理核心数据的系统，当满足四级以上网络安全等级保护和关键信息基础设施安全保护要求。

为了防止因意外等原因导致核心数据的丢失或损坏，应对核心数据进行备份。

核心数据所处的网络环境应与互联网物理隔离，严格监控核心数据的查看、查询、处理、传输、使用等状态，发现异常行为自动报警，并把报警信息第一时间发送给相关责任人和主管人员。

B.2 重要数据

根据《网络数据安全管理条例（征求意见稿）》，关于国家对重要数据进行重点保护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护，数据处理者应当使用密码对重要数据进行保护等规定，《数据安全法》关于重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告等规定，以及生态环境行业主管部门的有关规定，雄安新区生态环境局重要数据管控要求为：

为保障重要数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，维护数据的完整性、保密性、可用性，应对重要数据进行备份，重要数据传输、存储均使

用普通密码进行加密，无密码权限，任何人不能查看、处理和使用重要数据；限制重要数据超级管理员权限，对于重要数据删除、拷贝等可能导致数据丢失、泄露等安全隐患的操作，建立由数据处理者、数据直接负责人和主管领导三级审核机制，审核通过才能完成相关数据库操作。

处理重要数据的系统，当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求。

重要数据所处的网络环境应与互联网逻辑隔离，通过态势感知等技术手段，开展数据安全风险监测，严密监控重要数据的查看、查询、处理、传输、使用等状态，以及病毒、木马、后门等网络威胁攻击行为，发现异常行为自动报警，并把报警信息第一时间发送给相关责任人和主管人员，相关责任人第一时间对异常行为进行排查和处理，并根据严重程度，启动应急预案，并定期开展重要数据安全事件应急演练。

对于重要数据，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报河北省网信部门，年度数据安全评估报告的内容包括：处理重要数据的情况；发现的数据安全风险及处置措施；数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；落实国家数据安全法律、行政法规和标准情况；发生的数据安全事件及其处置情况；共享、交易、委托处理、向境外提供重要数据的安全评估情况；数据安全相关的投诉及处理情况；国家网信部门和主管、监管部门明确的其他数据安全情况。数据风险评估报告至少保持三年。

开展共享、交易、委托处理、向境外提供重要数据的安全评估，应当重点评估以下内容：共享、交易、委托处理、向境外提供数据，以及数据接收方处理数据的目的、方式、范围等是否合法、正当、必要；共享、交易、委托处理、向境外提供数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；数据接收方的诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险。评估认为可能危害国家安全、经济发

展和公共利益，不得共享、交易、委托处理、向境外提供数据。

重要数据发生数据安全事件对个人、组织造成危害的，应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人。

发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，应该在发生安全事件的八小时内向河北省网信部门和网络安全主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等；在事件处置完毕后五个工作日内向河北省网信部门和网络安全主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。

据处理者向第三方共享、交易、委托处理重要数据的，要与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

制定重要数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

重要数据的共享、交易、委托处理，应当征得河北省省级及以上数据安全主管部门同意。

重要数据出境，应当具备下列条件之一：需通过国家网信部门组织的数据出境安全评估；数据提供方和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证；按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务；存留相关日志记录和数据出境审批记录三年以上。

向境外提供重要数据，应当在每年 1 月 31 日前编制数据出境安全报告，向河北省数据安全主管部门报告上一年度以下数据出境情况：全部数据接收方名称、联系方式；出境数据的类型、数量及目的；数据在境外的存放地点、存储期限、使用范围和方式；涉及向境外提供数据的用户投诉及处理情况；发生的数据安全事件及其处置情况；数据出境后再转移的情况；国家网信部门明确向境外提供数据需要报告的其他事项。

B.3 一般数据

根据《网络数据安全管理条例（征求意见稿）》，关于国家对个人信息进行重点保护等规定，以及《个人信息保护法》关于任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动等规定，以及生态环境行业主管部门的有关规定，雄安新区生态环境局一般数据管控要求为：

任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息；个人信息收集，不应以欺诈、诱骗、误导的方式，收集个人信息；不应从非法渠道获取个人信息。

为保障一般数据中的个人信息免遭泄露、窃取、篡改、毁损、丢失、非法使用，维护数据的完整性、保密性、可用性，应对一般数据中的个人信息数据进行备份，数据传输、存储均使用商用密码进行加密，无密码权限，任何人不能查看、处理和使用个人信息；对于个人信息删除、拷贝等可能导致数据丢失、泄露等安全隐患的操作，建立由数据处理者、数据直接负责人和主管领导三级审核机制，审核通过才能完成相关数据库操作。

一般数据中的个人信息的系统，当满足三级以上网络安全等级保护要求，定期开展一般数据中的个人信息数据安全事件应急演练。

一般数据中的个人信息所处的网络环境应与互联网逻辑隔离，通过态势感知等技术手段，开展数据安全风险监测，严密监控重要数据的查看、查询、处理、传输、使用等状态，系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全风险行为，发现异常行为自动报警，并把报警信息第一时间发送给相关责任人和主管人员，相关责任人第一时间对异常行为进行排查和处理，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向雄安新区数据安全主管部门报告，并留存相关的网络日志不少于六个月。

数据安全事件对个人、组织造成危害的，应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人。

向第三方提供个人信息，应当向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的

不需要取得个人同意的情形或者经过匿名化处理的除外；与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；留存个人同意记录及提供个人信息的日志记录至少五年。

处理个人信息，应当具有明确、合理的目的，遵循合法、正当、必要的原则。基于个人同意处理个人信息的，应当满足以下要求：处理的个人信息是提供服务所必需的，或者是履行法律、行政法规规定的义务所必需的；限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式；不得因个人拒绝提供服务必需的个人信息以外的信息，拒绝提供服务或者干扰个人正常使用服务。

处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。个人信息处理规则应当包括但不限于以下内容：依据产品或者服务的功能明确所需的个人信息，以清单形式列明每项功能处理个人信息的目的、用途、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人的影响；个人信息存储期限或者个人信息存储期限的确定方法、到期后的处理方式；个人查阅、复制、更正、删除、限制处理、转移个人信息，以及注销账号、撤回处理个人信息同意的途径和方法；以集中展示等便利用户访问的方式说明产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称，以及每个第三方代码、插件收集个人信息的目的、方式、种类、频次或者时机及其个人信息处理规则；向第三方提供个人信息情形及其目的、方式、种类，数据接收方相关信息等；个人信息安全风险及保护措施；个人信息安全问题的投诉、举报渠道及解决途径，个人信息保护负责人联系方式。

处理个人信息应当取得个人同意的，并遵守以下规定：按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意；处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意；需向个人告知处理敏感个人信息的必要性以及对个人权益的影响；处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；不得以改善服务质量、提升用户体验、研发新产品等为由，强迫个人同意处理其个人信息；不得通过误导、欺诈、胁迫等方式获得个人的同意；不得通过捆绑不同类型

服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意；不得超出个人授权同意的范围处理个人信息；不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。

有下列情况之一的，应当在十五个工作日内删除个人信息或者进行匿名化处理：已实现个人信息处理目的或者实现处理目的不再必要；达到与用户约定或者个人信息处理规则明确的存储期限；终止服务或者个人注销账号；因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息；删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处理，并应当向个人作出合理解释。

个人提出查阅、复制、更正、补充、限制处理、删除其个人信息的合理请求的，应当提供便捷的支持个人结构化查询本人被收集的个人信息类型、数量等的方法和途径，不得以时间、位置等因素对个人的合理请求进行限制；提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件；收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权同意或者注销账号申请的，应当在十五个工作日内处理并反馈。

符合下列条件的个人信息转移请求，应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务：请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息；请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息；能够验证请求人的合法身份。数据处理者发现接收个人信息的其他数据处理者有非法处理个人信息风险的，应当对个人信息转移请求做合理的风险提示；请求转移个人信息次数明显超出合理范围的，数据处理者可以收取合理费用。

一般数据数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。

一般数据出境，应当具备下列条件之一：需通过国家网信部门组织的数据出境安全评估；数据提供方和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证；按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务。

向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意；个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。

向境外提供个人信息，应当在每年 1 月 31 日前编制数据出境安全报告，向雄安新区数据安全主管部门报告上一年度以下数据出境情况：全部数据接收方名称、联系方式；出境数据的类型、数量及目的；数据在境外的存放地点、存储期限、使用范围和方式；涉及向境外提供数据的用户投诉及处理情况；发生的数据安全事件及其处置情况；数据出境后再转移的情况；国家网信部门明确向境外提供数据需要报告的其他事项。

发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；个人信息处理者的联系方式。

附录 C 数据分类分级信息

一般数据填写基本情况和数据处理情况，重要数据和核心数据还需填写数据责任主体情况。

填报单位：		填报人：		联系方式：	

数据基本情况																数据处理情况				数据责任主体情况				备注	数据目录名称修改建议
数据目录（一级）	数据目录（二级）	数据目录（三级）	数据目录（四级）	数据名称	数据级别	数据载体	数据来源	数据数量	数据精度			详细描述	所属信息系统			数据处理单位	数据所属主管部门	数据处理活动方式	数据是否跨主体流动	是否涉外	是否出境	数据处理单位主要负责人	本项数据安全负责人	本项数据安全负责人联系方式	数据所属地区		
									地域范围	时间范围	更新周期		系统名称	是否属于关键信息基础设施	网络安全等级保护级别												
选择	选择	选择	选择	填写	选择	选择	多选	填写	填写	填写	选择	填写	填写	选择	选择	选择	选择	多选	选择	选择	选择	填写	填写	填写	填写	填写	填写

填表说明：

数据目录（一级）：在 21 个一级目录中选择；

数据目录（二、三、四级）：在二、三、四级目录中选择，如需新增，需手动添加，如有修改建议，在“数据目录名称修改建议”栏填写；

数据名称：填写数据具体名称；

数据级别：选择数据级别，包括一般数据、重要数据、核心数据；

数据载体：选择数据载体，包括电子数据、纸质数据、其他，选择其他，需说明具体载体形式；

数据来源：选择数据的获取渠道，包括机器采集、手工采集、数据共享、公开数据库、出版物，其他等，选择其他需说明数据具体获取渠道，可多选；

数据数量：填写数据容量（单位为 TB、GB、MB）或数据条数（单位为条）

地域范围：填写数据所涉及的地域范围；

时间范围：填写数据所涉及的时间范围；

更新周期：选择数据更新时间或频率，包括实时、每分钟、每小时、每天、每周、每月、每季度、每年、不定期、其他等，选择其他需说明具体更新周期；

详细描述：填写数据的具体内容、用途等；

系统名称：填写数据所属信息系统的名称；

是否数据关键信息基础设施：选择数据所属信息系统是否属于关键信息基础设施；

网络安全等级保护级别：选择数据所属信息系统评定的网络安全保护等级；

数据处理单位：选择开展数据处理活动的机关部门或厅属单位名称；

数据所属主管部门：选择数据所属业务主管部门名称；

数据处理活动方式：选择数据处理活动方式，包括收集、存储、使用、加工、传输、提供、公开，可多选；

是否跨主体流动：选择数据是否跨主体流动；

是否涉外：选择数据是否涉及境外，如涉及境外，需说明具体情况；

是否出境：选择数据是否出境，如涉及出境，需说明数据去向。

数据处理单位主要负责人：填写开展数据处理活动单位的主要负责人姓名；

本项数据安全负责人：填写开展数据处理活动单位中，本项数据安全负责人姓名；

本项数据安全负责人联系方式：填写本项数据安全负责人联系电话；

单位所属地区：填写开展数据处理活动单位所在直辖市或地级城市名称；

备注：填写需对该数据目录的补充说明；

数据目录名称修改建议：填写对相关数据目录名称的修改建议。

参 考 文 献

[1]《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）

[2]《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）

[3]《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释[2017〕10号）

[4]《网络安全审查办法》（国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局令第8号）

[5]《网络数据安全管理条例（征求意见稿）》

[6]《中华人民共和国个人信息保护法》（中华人民共和国主席令第九十一号））