江苏省生态环境数据分类分级管理规范
（试行）

第一章 总则

第一条 为加强生态环境数据安全保护，规范数据安全有序运行管理，依据《江苏省公共数据管理办法》《江苏省公共数据分类分级规范》等文件要求，结合本省生态环境工作实际，制定本规范。

第二条 本省行政区域内生态环境数据的分类分级管理适用本规范。法律、法规另有规定的，从其规定。

本规范所称数据，是指本省各级生态环境部门在依法履行职责、推进业务管理、开展环境监测、科学研究等日常工作中获取和加工的各类生态环境数据，以及对生态环境数据开发利用形成的数据成果或产品。涉及国家秘密的数据不包含在本规范管理范围之内。

生态环境数据分类分级管理应当遵循合法合规、科学系统、准确实用、就高从严的原则。

第三条 厅网络安全与信息化领导小组统筹负责省生态环境数据分类分级工作的组织、协调和监督。厅网络安全与信息化领导小组办公室设在省生态环境监控中心，负责制定并动态调整全

省生态环境数据的分类与分级框架及标准规范，并对全省生态环境数据的分类与分级方法落地实施开展考核，对配合不力的部门（单位）予以通报。厅各部门（单位）、各设区市生态环境局及其他数据生产单位，负责判定本单位数据资源的分类分级。各设区市生态环境局应当在全省数据分级分类框架下细化调整本单位数据分类分级规范。

第二章 数据分类管理

第四条 应根据数据来源、形式、用途等，对生态环境数据进行分类管理。

第五条 应按照系统性、扩展性、准确性、实用性和时效性统筹兼顾的原则，对生态环境数据进行管理。

第六条 生态环境数据分为环境质量信息、生态环境信息、污染源信息、环境管理业务信息等10个大类，每个大类根据管理需要可分为若干中类及小类（具体分类名录见附件1）。

第七条 各设区市生态环境局须按照分类标准及相应规范要求，对数据进行分类。如有特殊情况的，可根据需要新增中类和小类，增设后数据分类管理代码赋码等需报省生态环境厅同意后执行。

第三章 数据分级管理

第八条 根据数据重要程度，以及一旦遭到篡改、破坏、泄露

或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对生态环境数据进行定级。

第九条 生态环境数据分为四个等级：一级为不敏感数据，二级为低敏感数据，三级为敏感数据，四级为高敏感数据（数据分级方法见附件 2）。未进行分级的数据由数据产生单位定级，并向省生态环境厅报备。数据定级完成后，省生态环境厅根据实际情况，可不定期对分级表进行变更。

第十条 对于一级数据，在做好安全管理基础上应对公众无条件开放，并支持各地、各部门无条件共享。一级数据应尽可能通过各地政府及生态环境部门网站、微信公众号等渠道进行公开发布。

第十一条 对于二级数据，符合法律法规要求，可以共享、公开的应全部进行共享、公开，不得人为设置障碍。在共享、公开时应遵循以下要求：

（1）申请共享、公开数据的单位和个人应向生态环境管理部门提供正式申请，说明数据使用目的、用途和范围；生态环境机关经评估，确认数据共享、开放不产生轻微以上影响，对数据安全可控后可批准数据共享、开放。

（2）数据应仅限申请人使用，不得进行二次传播。

（3）数据传输过程应通过可控渠道进行，原则上不通过互联网传播。

（4）需要脱敏的数据，应在脱敏后再进行共享、公开。

（5）生态环境管理部门应对共享、开放过程进行日志记录和审计。

（6）申请人数据使用结束即采用删除、覆盖或格式化方式销毁数据，对销毁过程有审批、记录、监督。

第十二条 对于三级数据，进行严格的管理监督。三级数据审慎进行共享、开放，在执行第十三条管理规定的基础上，增加以下要求：

（1）在收到正式共享、开放申请后，生态环境部门经评估，确认数据共享、开放不产生一般以上影响，对数据安全可控后可批准数据共享、开放。

（2）数据传输过程应通过光盘等完全安全可控方式进行，不可通过互联网传输。

（3）应对数据进行必要脱敏处理。

（4）业务结束即以不可逆方式销毁数据，对销毁过程有审批、记录、监督。

第十三条 对于四级数据，进行最严格的管理监督，禁止开放，原则上不予共享。特殊条件确需共享时，在执行第十四条管理规定的基础上，需要通过专家委员会一事一议，对共享方式、流程、技术细节进行确认形成共享方案后，再进行共享。

第四章 数据安全管控

第十四条 对不同级别数据根据其数据生命周期进行差异化

安全管控，按照采集、传输、存储、处理、共享、开放、销毁等阶段实施数据生命周期分级管控（管控具体要求见附件3）。

第五章 监督与保障

第十五条 省生态环境厅在省大数据管理中心指导下，开展全省生态环境数据分类分级管理监督工作。

第十六条 省生态环境厅组织各地生态环境管理部门落实好数据安全管理工作，深化网络安全等级保护要求，制定数据安全应急预案，组织开展安全演练。发生数据安全事件时，应立即按要求上报，并做好事件预警与应急响应处置工作。

第十七条 各地生态环境管理部门对各自负责管理的数据实行全生命周期安全管控，严格落实管控要求，设置专职岗位和人员，落实与管理数据级别数量相匹配的机制、措施、技术、工具，确保生态环境数据实现全生命周期安全可控。

第十八条 各级生态环境管理部门应将数据分类分级工作纳入绩效管理，制定考核评价机制，对管理工作成效进行评价。

第六章 附则

第十九条 涉及国家秘密信息、密码使用的数据活动，按照国家有关规定执行。

第二十条 本规范由厅网络安全与信息化领导小组办公室负责解释。

第二十一条 本规范自发布之日起施行。

附件 1

生态环境数据分类目录

代码	类目名称	备注
01	**环境质量信息**	
0101	环境功能区划	
0102	环境质量数据	指通过监测、调查等获取的基础数据
0103	环境质量报告	指对环境质量基础数据整理、分析和评价的结果
0104	环境质量点位信息	
0199	其他环境质量信息	
02	**生态环境信息**	包括生态环境的基础数据及其整理、分析和评价的结果（如生态环境质量评价等）
0201	自然生态	
0202	农村生态	
0203	生物多样性	
0204	生物安全	
0299	其他生态环境信息	
03	**污染源信息**	包括污染源基本信息、生产状况、能源及原材料消耗、污染物排放、治理设施等信息
0301	工业污染源	包括污染源监测/调查/分析报告等信息
0302	农业污染源	
0303	生活污染源	
0304	交通运输污染源	
0305	施工工地污染源	
0306	服务业污染源	
0307	集中式污染治理设施	
0308	环境污染危险源信息	
0309	污染物信息	
0310	碳排放信息	
0399	其他污染源信息	包括内源（如底泥等）、水土流失、大气输移等形成的污染源，以及入河/湖/库/海排污口和其他污染源信息
04	**环境管理业务信息**	
0401	规划计划	

代码	类目名称	备注
0402	环境管理制度	
0403	污染防治	
0404	生态环境保护与修复	
0405	核与辐射安全管理	包括核与辐射安全管理（污染预防）、污染防治及其他相关信息
0406	环境污染事故与应急管理	包括水环境、海洋环境、大气环境、声环境的污染，生态破坏以及核与辐射污染事故及应急管理
0407	监测/检测管理	
0408	环境监察	
0409	环境行政处罚、行政复议和诉讼	环境行政处罚、行政复议和诉讼工作过程产生的信息
0410	国际合作与交流	
0411	环境专业人才管理认证	
0412	环境公众参与	
0413	环境宣传教育	
0414	环境信息管理	
0499	其他环境管理业务信息	
05	**环境科技及其管理信息**	
0501	环境科技信息	可根据《中国图书馆分类法详表》进行更详细的分类
0502	环境科技管理	
0503	环境认证管理	
0599	其他环境科技信息	
06	**环境保护产业信息**	
0601	环境保护产品信息	包括环境保护仪器、设备等
0602	环境保护产业项目	
0603	环境保护产业组织	
0604	环境保护技术转化与推广	
0605	环境保护工程设计	
0606	环境保护产业园区	
0607	环境保护产业服务	
0608	环境保护设施运营	
0609	环境保护计量认证	

代码	类目名称	备注
0610	环境保护检测机构认可	
0611	清洁生产	
0612	循环经济	
0699	其他环境保护产业信息	
07	**环境政务管理信息**	
0701	机构人事管理	
0702	文档管理	
0703	日常政务信息	
0704	政务督查	
0705	资产管理	
0706	个人办公	
0707	会议管理	
0708	财务管理	指非规划相关的财务管理，涉及财务核算、资金收支、财务信息和财务监督等环节，包括收费项目、标准、依据、范围、程序等内容
0709	值班管理	
0710	党建管理	
0711	纪检监督	
0712	保密工作管理	
0713	接待管理	
0714	后勤管理	
0799	其他环境政务管理信息	
08	**环境政策法规标准**	
0801	环境政策法规	
0802	环境标准	
0899	其他环境政策法规标准	
09	**环境保护相关信息**	注：此类目下的信息为环保系统以外的部门直接采集的信息
0901	自然环境信息	
0902	社会经济信息	
0999	其他环境保护相关信息	
99	**其他环境信息**	

附件 2

生态环境数据分级方法

根据数据影响程度和分级判定标准，对库表、文件、接口存储和传输的数据做定级。对于没有分级的公共数据，暂时不予开放，待确定等级之后安全有序开放。

表 1　影响程度说明表

影响程度	参考说明
严重影响	1．可能导致危及国家安全的重大事件，发生危害国家利益或造成重大损失的情况。 2．可能导致严重危害社会秩序和公共利益，对全社会、多个行业、行业内多个组织或者大量人民群众造成严重影响。 3．可能对组织的正常运作造成严重影响，导致大部分甚至全部业务无法正常开展，资产、形象和声誉受到严重损害。 4．可能对个人合法权益造成严重程度影响，导致人身安全、财产安全、精神状况、人格尊严、个人名誉等出现严重损害。 以上损害结果不可逆。
一般影响	1．可能导致危害社会秩序和公共利益，对部分行业、部分组织或者部分人民群众造成影响。 2．可能对组织正常运作造成一般程度影响，导致重要或关键业务无法正常开展、资产、形象和声誉受到损害。 3．可能对个人合法权益造成一般程度损害，导致人身安全、财产安全、精神状况、人格尊严、个人名誉等出现损害。 以上损害结果不可逆，但可以采取一些措施降低损失。
轻微影响	1．可能导致轻微危害社会秩序和公共利益，对个别行业、个别组织或者个别人民群众造成轻微影响。 2．可能对组织正常运作造成轻微影响，导致重要/关键业务出现中断、资产、形象和声誉受到轻微损害。 3．可能对个人的合法权益造成轻微影响，导致人身安全、财产安全、精神状况、人格尊严、个人名誉等出现轻微损害。 以上损害结果可被补救或者补偿。

无影响	对国家安全、公共利益、组织合法权益和个人合法权益等不造成损害。

表 2　生态环境数据分级判定标准表

安全等级	敏感程度	影响程度	共享属性	开放属性
四级	高敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后造成严重影响。	严格条件共享/不与共享	不予开放
三级	敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后造成一般影响。	严格条件共享	严格条件开放/不予开放
二级	低敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后造成轻微影响。	一般条件共享	一般条件开放
一级	不敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后无影响。	无条件共享	无条件开放

已合法公开披露的公共数据可定为一级；法律法规规章未明确要求公开的个人信息等级不得低于二级；法律法规明确要求保护的公共数据，数据安全等级应定为三级以上；其他数据根据影响程度和分级判定标准自主定级。

对于在库表和数据文件中存储的数据分级标记应细化至数据的字段级，相关库表、文件的级别按照包含字段的最高安全级别定级。

对数据接口定级按照其响应请求返回字段中安全级别最高的字段级别定级。

对有数据融合场景的数据应用，注意根据数据融合风险对数据定级，应结合场景、数据可整合关联出的信息综合判定数据级别，因数据整合应用产生更高级别的敏感度的情况下，按照高级别的敏感度定级。对于无法评估的不确定性风险，建议通过组织行业专家座谈研讨等方式确定公共数据级别。

附件 3

生态环境数据分级管控具体要求

一、数据采集管控

（一） 一级数据管控

1．生态环境数据采集应遵循合法、正当、必要和诚信原则。数据采集需有明确的目的、用途和范围。各类生态环境质量监测数据获取应符合相应规范，在线监控数据仪器设备、运行状况等需符合相应要求，其他数据采集流程和方法也需合理合法。

2. 应明确数据的最小颗粒度到具体字段级别，对采集账号权限管理，根据对数据字段的需求，依据权限最小化原则分配采集账号权限，并通过管控实现账号认证和权限分配，不得采集提供服务所必需以外数据。

3. 各类生态环境数据的采集渠道均需清晰明确，需要从外部渠道采集（输入）数据的，应对数据来源合法性、数据真实性进行确认。

4. 坚持“一数一源”，一个数据只能有一个提供者。对于同一项数据可能来自多源的情况，应对数据分类区分，或进行多源比对及校正后再进行取值。

5．对各类生态环境数据，应根据其来源不同，分别建立合理的数据采集流程。针对在线的数据采集过程执行有效的日志记录，对数据流量实施限流控制。线下采集的数据，存储介质要经过安

全扫描、病毒查杀确认安全之后再进行数据的采集使用。

6.采集设备接入管理，对采集设备 IP 地址、Console、USB 端口访问进行限制，对采集设备接入进行认证鉴权。

（二） 二级数据管控

在满足一级管控要求基础上，还需满足以下要求。

1. 采取必要的技术手段对采集的数据进行校验，以保证其完整性和一致性。

2. 宜实施数据采集过程的数据防泄漏安全技术措施，防止数据在采集过程中的泄露，如数据加密、采集链路加密、敏感字段脱敏等。

（三） 三级数据管控

在满足二级管控要求基础上，还需满足以下要求。

1. 待采集数据采取数据访问控制等保护措施。

（四） 四级数据管控

在满足三级管控要求基础上，还需满足以下要求。

1. 应对外部收集的数据和数据源进行识别和记录，即通过数据溯源的机制保证数据管理人员能够追踪其加工和计算的数据来源。

二、数据传输管控

（一） 一级数据管控

1. 加强数据线下交互的过程管控，对数据线下交互建立审批机制及操作流程，要求对线下交互数据采取加密、脱敏、物理封

装等防护手段，防止数据被违规复制、传播、破坏等。

2. 在网络边界上针对数据流向做好隔离封堵的限制。

3. 能够校验数据在传输过程中完整性。

（二） 二级数据管控

在满足一级管控要求基础上，还需满足以下要求。

1. 应建立安全的数据传输通道，例如 VPN、专线等。

2. 应对数据进行来源正确性检测。

3. 应对传输通道两端进行主体身份鉴别和认证。

（三） 三级数据管控

在满足二级管控要求基础上，还需满足以下要求。

1. 应对数据进行加密传输。加密算法应符合国家密码管理的相关法律法规要求。

（四） 四级数据管控

在满足三级管控要求基础上，还需满足以下要求。

1. 应使用数据溯源（如水印溯源）等技术，对数据泄露风险及行为进行追踪，如定位到责任人等。

三、数据存储管控

（一） 一级数据管控

1. 生态环境数据应保存在可信或可控的信息系统或物理环境中。

2. 应对存储系统的账号权限进行最小权限管理。

3．应建立本地数据备份与恢复机制，定期进行数据的备份。

（二） 二级数据管控

在满足一级管控要求基础上，还需满足以下要求。

1. 公共应对存储系统的访问进行鉴权、日志记录、审计。

2. 硬件冗余，保证系统高可用性。

3. 建立数据异地备份与恢复机制，定期进行数据的备份。

（三） 三级数据管控

在满足二级管控要求基础上，还需满足以下要求。

1. 重要的敏感数据应进行加密存储。

2. 建立数据实时备份机制。

（四） 四级数据管控

在满足三级管控要求基础上，还需满足以下要求。

1. 应建立异地灾备中心，提供业务应用的实时无缝切换。

四、数据处理管控

（一） 一级数据管控

1. 设置身份标识与鉴别机制。

2. 对数据操作行为进行日志记录、审计与分析。

3. 依据权限最小化原则分配账号权限，通过管控技术手段统一实现账号认证和权限分配；不同用户只能访问与自己职责对应的数据。

4．应建立数据分析挖掘的操作过程、输出结果的安全审查、合规风险评估和数据使用授权流程。

5. 对于系统间和后台数据的转移、导出行为，应通过管理和

技术手段予以严格控制。

（二） 二级数据管控

在满足一级管控要求基础上，还需满足以下要求。

1. 供开发人员使用的测试数据必须经过模糊化处理。

2. 对获取数据和本地下载等的敏感操作行为，应进行二次操作审批。

（三） 三级数据管控

在满足二级管控要求基础上，还需满足以下要求。

1. 应采用口令、密码、生物识别等两种以上鉴别技术同时对用户进行身份鉴别。

2. 对敏感数据访问应进行模糊化或脱敏处理。

3. 数据进行对外查询、展现、统计等操作时，必须经过模糊化处理。

4. 介质中的数据必须进行加密保护。

（四） 四级数据管控

在满足三级管控要求基础上，还需满足以下要求。

1．需要满足多人操作管理，确保单人无法拥有重要数据的完整操作权限。

2. 应持续对账号进行风险监控，动态授权。

五、数据共享管控

（一） 一级数据管控

1. 建立数据共享目录，明确数据的共享范围和使用属性。

2. 无条件共享。

（二） 二级数据管控

1. 应建立数据共享目录，明确数据的共享范围和使用属性。

2. 对共享数据的使用申请进行严格审批和授权。

3. 建立数据共享的唯一通道，定义数据共享的字段、传输方式、服务接口，并对数据共享过程进行日志记录和审计。

（三） 三级数据管控

在满足二级管控要求基础上，还需满足以下要求。

1. 数据共享前应进行脱敏处理。

2. 对数据共享全链路各环节风险进行监控。

（四） 四级数据管控

在满足三级管控要求基础上，还需满足以下要求。

1. 一般情况不允许共享。

2. 若需共享应采取一事一议制，经相关责任人审批授权，进行脱敏降级后共享。

六、数据开放管控

（一） 一级数据管控

1. 建立数据开放目录，明确数据的开放范围和使用属性。

2. 无条件开放。

（二） 二级数据管控

1. 建立数据开放目录，明确数据的开放范围和使用属性。

2. 生态环境管理部门审批后有条件开放。

3. 根据需求场景情况对安全风险较高场景实施数据脱敏。

4. 应对开放数据实时监控，发现频繁查询请求、抓取等异常动作时对请求阻断。

（三） 三级数据管控

在满足二级管控基础上，还需满足以下要求。

1. 对数据开放全链路各环节的权限最小化控制，如进行白名单控制；记录请求访问日志；对异常进程监控。

（四） 四级数据管控

第四级数据禁止开放。

七、数据销毁管控

（一） 一级数据管控

1. 建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。

2. 业务终止时自行决定数据是否需要销毁，宜采用删除、覆写法等方式进行数据销毁。

（二） 二级数据管控

1. 建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制。

2. 业务终止时采用删除、覆写法等方式销毁有关数据。

（三） 三级数据管控

1. 建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制。

2. 应以不可逆的方式销毁有关数据。可使用国家权威机构认证的设备对存储介质进行销毁，或联系专业机构执行销毁工作。

（四） 四级数据管控

同第三级管控要求。