自然资源领域数据安全管理办法

第一章　总则

第一条 为规范自然资源领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》等法律法规，制定本办法。

第二条　在中华人民共和国境内开展的，或在境外履行自然资源部门职责过程中开展的自然资源领域非涉密数据处理活动及其安全监管，应当遵守相关法律法规和本办法的要求。

第三条　本办法所称自然资源领域数据，是指在开展自然资源活动中收集和产生的数据，主要包括基础地理信息、遥感影像等地理信息数据，土地、矿产、森林、草原、水、湿地、海域海岛等自然资源调查监测数据，总体规划、详细规划、专项规划等国土空间规划数据，用途管制、资产管理、耕地保护、生态修复、开发利用、不动产登记等自然资源管理数据。

本办法所称自然资源领域数据处理者（以下简称数据处理者），是指开展自然资源领域数据处理活动的自然资源行业各类单位。

本办法所称数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态

的能力。

第四条　在国家数据安全工作协调机制统筹协调下，自然资源部承担自然资源行业、领域数据安全监管职责，负责督促指导各省、自治区、直辖市自然资源主管部门、海洋主管部门（以下统称地方行业监管部门）开展数据安全监管。国家林业和草原局具体承担森林草原、湿地荒漠等数据安全监管职责，参照本办法制定具体制度。

地方行业监管部门分别负责对本地区自然资源领域数据处理活动和安全保护进行监督管理。

自然资源部、国家林业和草原局及地方行业监管部门统称为行业监管部门。

行业监管部门将数据安全纳入党委（党组）国家安全责任制，按照“谁管业务，谁管数据，谁管数据安全”原则，落实本行业本地区本领域数据安全指导监管责任。

第五条　自然资源部、国家林业和草原局推进自然资源领域数据开发利用和数据安全标准体系建设，组织开展相关标准制修订及推广应用。

第六条　鼓励自然资源领域数据依法共享开放和开发利用，支持数据创新应用。积极构建数据开发利用和安全产业协调共进的发展模式，不断提升数据安全保障能力，维护国家安全、社会稳定、组织和个人权益。

第七条　支持开展经常性的自然资源领域数据安全宣传教育。采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第二章　数据分类分级管理

第八条　自然资源部组织制定自然资源领域数据分类分级、重要数据和核心数据识别认定、数据安全保护等标准规范，指导开展数据分类分级管理工作，编制行业重要数据和核心数据目录并实施动态管理。国家林业和草原局按照自然资源领域数据分类分级标准规范，结合工作需要编制林草领域数据安全标准规范，指导开展林草数据分类分级工作，编制林草重要数据和核心数据目录并实施动态管理。

地方行业监管部门按照自然资源领域数据分类分级标准规范,分别组织开展本地区自然资源领域数据分类分级管理及重要数据和核心数据识别审核工作，编制本地区自然资源领域重要数据和核心数据目录，并上报自然资源部，目录发生变化的，应及时上报更新。

数据处理者应当定期按照自然资源领域数据分类分级标准规范梳理填报重要数据和核心数据目录。

第九条　根据行业特点和业务应用，自然资源领域数据分类类别包括但不限于地理信息、自然资源调查监测、国土空间规划、自然资源管理等，具体参照自然资源领域数据分类分级标准规范。

通过对自然资源领域数据重要性、精度、规模、安全风险，以及数据价值、可用性、可共享性、可开放性等进行综合分析，判断数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围进行分级，分为一般数据、重要数据、核心数据。

数据处理者可在此基础上细分数据的类别和一般数据级别。

第十条　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。核心数据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，经国家有关部门评估确定的其他数据。

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，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

一般数据是指除重要数据、核心数据以外的其他数据。

结合自然资源领域数据特点，满足以下两项（含）以上参考指标的为重要数据。

（一）支撑党中央和国务院赋予的“两统一”职责产生的具有不可替代性和行业唯一性的，一旦发生数据篡改、泄露或服务中断等安全事故，将影响自然资源部门履行职责，对全国范围内服务对象产生重要影响的数据。

（二）涉及国民经济和重要民生的，为其他行业、领域提供自然资源基础数据支撑的，一旦发生数据安全事故会对其他行业、领域造成重要影响的数据。

（三）覆盖多个省份甚至全国，规模大、精度高，且极具敏感性、重要性的数据。

（四）直接影响国家关键信息基础设施正常运行服务的数据。

（五）危害国家安全、国家经济竞争力、危害公众接受公共服务、危害公民生存条件和安定工作生活环境、危害公民的生命财产安全和其他合法利益、导致社会恐慌等的数据。

（六）我国法律法规及规范性文件规定的其他自然资源重要数据。

符合重要数据指标，且关系国家经济命脉、重要民生和重大公共利益、影响政治安全的数据为核心数据。

第十一条　自然资源部所属的数据处理者应当将本单位重要数据和核心数据目录向自然资源部报备，国家林业和草原局所属的数据处理者应当将本单位重要数据和核心数据目录向国家林业和草原局报备，其他数据处理者应当将本单位重要数据和核心数据目录向本地区行业监管部门报备。报备内容包括但不限于数据类别、级别、规模、精度、来源、载体、使用范围、对外共享、跨境传输、 安全情况及责任单位情况等，不包括数据内容本身。

地方行业监管部门应当在数据处理者提交报备申请后的二十个工作日内完成审核工作，报备内容符合要求的，报自然资源部审核认定，自然资源部接到申请后二十个工作日完成重要数据认定，核心数据须报国家数据安全工作协调机制认定；不符合要求的应当及时反馈申请单位并说明理由。申请单位应当在收到反馈后的十五个工作日内再次提交申请。

报备内容发生重大变化的，数据处理者应当在发生变化的三个月内履行变更手续。重大变化是指数据内容发生变化导致原有级别不再适用的，或某类重要数据和核心数据规模变化30%以上的，等等。

第三章　数据全生命周期安全管理

第十二条　数据处理者应当对数据处理活动安全负主体责任，对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。

（一）建立数据安全管理制度，针对不同级别数据，制定数据全生命周期各环节的具体分级防护要求和操作规程。

（二）根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业监管部门开展工作。

（三）利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求。

（四）应当采取相应技术措施和其他必要措施保障数据安全，防范数据被篡改、破坏、泄露或者非法获取、非法利用等风险。

（五）合理确定数据处理活动的操作权限，严格实施人员权限管理。

（六）根据应对数据安全事件的需要，制定应急预案，并开展应急演练。

（七）定期对从业人员开展数据安全知识和技能相关教育培训。

（八）法律法规等规定的其他措施。

重要数据和核心数据处理者，还应当：

（一）建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，建立常态化沟通与协作机制。本单位法定代表人或主要负责人是数据安全第一责任人，领导班子中分管数据安全的班子成员是直接责任人，其他成员对职责范围内的数据安全工作负领导责任，履行数据安全保护义务，接受监督。

（二）明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容。应当按照业务工作需要和最小授权原则，依据岗位职责设定数据处理权限，控制重要数据接触范围，人员变动时应及时调整权限。涉及核心数据的相关关键岗位人员、信息系统建设和运维单位等，提交公安机关、国家安全机关进行国家安全背景审查。

（三）建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录不少于六个月。

（四）在数据全生命周期的各环节，应当综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护，并按照法律法规和国家有关规定要求使用商用密码进行保护。

（五）涉重要数据信息系统建设、运维项目未经委托方批准不得转包、分包。建设运维人员未经委托方明确授权，不得处理委托方的重要数据。在提供涉重要数据信息系统建设、运维过程中收集、产生的数据，不得用于其他用途，服务完成后按照与委托方约定处理或及时删除。

（六）应当加强人员和经费保障。

第十三条　数据处理者收集数据应当遵循合法、正当的原

则，不得窃取或者以其他非法方式收集数据。法律法规对收集数据的目的、范围有规定的，应当在法律法规规定的目的和范围内收集。

数据收集过程中，应当根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集生产人员、设备的管理，并对收集来源、时间、类型、数量、精度、区域、频度、流向等进行记录。

通过间接途径获取重要数据和核心数据的，数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

第十四条 数据处理者应当依据法律法规规定的方式和期限存储数据，可以从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面，加强数据存储安全管控，保障存储数据的完整性、保密性、真实性和可用性。

存储重要数据的，要落实第三级及以上网络安全等级保护要求。存储核心数据的，要落实关键信息基础设施安全保护要求或第四级网络安全等级保护要求。

第十五条 数据处理者开展数据加工使用处理活动，应当采取访问控制、数据防泄露、操作审计等管控措施，确保过程安全、合规、可控、可溯源，防范数据关联挖掘、分析过程中有价值信息和个人隐私泄露的安全风险，明确数据使用加工过程中的相关责任，保证数据的正当加工使用。加工使用过程中，应当按照数据级别采取相应的措施保护数据的安全性，所使用的数据必须是真实可靠的，数据来源、收集过程须经过审查和核实。涉及利用数据进行自动化决策的，应当保证决策的

透明度和结果公平合理。加工使用重要数据和核心数据，还应当实施严格的访问控制，建立数据可信可控、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等相关技术和管理机制。

第十六条　数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

第十七条　数据处理者应当按照有关规定安全有序提供数据，明确提供的范围、类别、条件、程序等，提供的数据应当限于实现数据接收方处理目的的最小范围，并告知数据接收方按照对应级别进行分类分级保护，采取必要的安全保护措施，涉及重要数据的，与数据接收方签订数据安全协议。重要数据在共享、调用过程中应当加强安全管控，采取技术措施定期监测数据共享、调用的情况，并配备风险隔离、认证鉴权、威胁告警等安全保护措施。涉及提供、共享核心数据的，应当采取必要的安全保护措施，并上报自然资源部，自本年度1月1日起可能累计达到总量30%及以上的，应当经自然资源部报国家数据安全工作协调机制组织风险评估。涉及国家机关依法履职或单位内部流动的除外。

第十八条　数据处理者应当在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在显著负面影响或风险的，不得公开。政府机关部门应当遵守公正、公平、便民的原则，按照规定及时、准确地公开政务数据，依法不予公开的除外。

第十九条　数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。依据法律法规规定、合同约定等请求销毁的，数据处理者应当销毁相应数据。

销毁重要数据和核心数据的，要采取必要的安全保护措施，并事前向行业监管部门报告数据销毁方案。引起重要数据和核心数据目录变化的，应当及时向行业监管部门报备，不得以任何理由、任何方式对销毁数据进行恢复。

第二十条　数据处理者在中华人民共和国境内收集和产生的重要数据，应当在境内存储，确需向境外提供的，数据处理者应当落实国家网信部门数据出境安全评估有关规定。

第二十一条　数据处理者因重组等原因需要转移数据的，应当明确数据转移方案。涉及重要数据的，应当采取必要的安全保护措施，事前向行业监管部门报告数据转移方案。引起重要数据目录发生变化的，应当及时向行业监管部门报备。

第二十二条　数据处理者委托他人处理、与他人共同处理数据的，数据安全责任不因委托而改变，应当通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务。涉及重要数据的，委托方要把安全作为重要考虑因素，应当对受托方的数据安全保护能力、资质进行评估或核实，经过严格的审批程序，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。

除法律法规等另有规定外，未经委托方同意，受托方不得将数据提供给第三方。

第二十三条　数据处理者应当在数据全生命周期处理过程

中，记录数据处理、权限管理、人员操作等日志，并采用商用密码技术保护日志的完整性。其中，一般数据的日志留存时间不少于六个月，涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于三年。涉及核心数据安全事件处置、溯源的相关日志留存时间不少于三年。

第四章　数据安全监测预警与应急管理

第二十四条　自然资源部按照国家相关标准和流程，组织建立自然资源领域数据安全风险监测机制，建立自然资源领域数据安全风险监测预警体系，划分数据安全风险和事件等级，组织建设数据安全监测预警技术手段，形成监测、溯源、预警、处置等能力，与相关部门加强信息共享。国家林业和草原局组织建立林草数据安全风险监测预警机制，划分林草数据安全风险和事件等级，组织建设林草数据监测预警技术手段。

地方行业监管部门分别建设本地区数据安全监测预警机制，组织开展本地区自然资源领域数据安全风险监测，按照有关规定及时发布预警信息，通知本地区数据处理者及时采取应对措施。

数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。

第二十五条　自然资源部组织指导开展自然资源领域数据安全风险评估等工作。国家林业和草原局组织指导开展林草数据安全风险评估等工作。

地方行业监管部门分别负责组织开展本地区自然资源领域数据安全风险评估工作。

重要数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向行业监管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的类别、数量，开展数据处理活动的情况，面临的数据安全风险、应对措施及其有效程度等。数据处理者应当保留风险评估报告至少三年。核心数据处理者优先使用第三方评估机构开展风险评估。

数据处理者在组织重要数据安全风险评估时，应当对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或异常行为，应及时采取相应处置措施。

第二十六条 自然资源部组织建立自然资源领域数据安全风险信息通报机制，统一汇集、分析、研判、通报数据安全风险信息。国家林业和草原局组织建立林草数据安全风险信息通报机制。

地方行业监管部门分别汇总分析本地区自然资源领域数据安全风险，根据数据安全风险的发展态势、规模大小、关联程度、现实危害等综合研判，及时将可能造成重大及以上安全事件的风险向自然资源部报告。

数据处理者及时将可能造成较大及以上安全事件的风险向行业监管部门报告。

第二十七条 自然资源部组织制定自然资源领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。国家林业和草原局组织建立林草数据安全事件应急预

案，组织协调重要数据和核心数据安全事件应急处置工作。

地方行业监管部门分别组织开展本地区自然资源领域数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即报自然资源部，并及时报告事件发展和处置情况。

数据处理者在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，第一时间向行业监管部门、属地公安部门报告，事件处置完成后在一周以内形成总结报告。每年向行业监管部门报告数据安全事件处置情况。

数据处理者对发生的可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

第五章　监督检查

第二十八条　行业监管部门对数据处理者落实数据分类分级保护及本办法要求的情况进行监督检查。数据处理者应当对行业监管部门监督检查予以配合。

第二十九条　在国家数据安全工作协调机制统一组织下，自然资源部依法配合有关部门，对影响或者可能影响国家安全的自然资源领域数据处理活动开展数据安全审查工作。

第三十条　数据处理者及其委托的数据安全风险评估机构工作人员对在履行职责中知悉的个人信息、商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

第六章　法律责任

第三十一条　行业监管部门在履行数据安全监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序对数据处理者进行约谈，并要求采取措施进行整改，消除隐患。

第三十二条　对于违反有关规定的，依照《中华人民共和国数据安全法》及有关法律法规予以处理，根据情节严重程度给与相应行政处罚，构成犯罪的，依法追究刑事责任。

第七章　附则

第三十三条　开展涉及个人信息的数据处理活动，还应当遵守有关法律法规的规定。

第三十四条　涉及国家秘密信息或自然资源领域数据汇聚关联后属于国家秘密事项的数据处理活动，应当符合国家及部相关保密规定。

第三十五条　法律法规规定开展数据处理活动应当取得行政许可的，数据处理者应当依法取得许可。

第三十六条　本办法由自然资源部负责解释。

第三十七条　本办法自印发之日起施行。