附件 1

工业和信息化领域数据安全管理办法（试行）

（公开征求意见稿）

第一章 总则

第一条【目的依据】为规范工业和信息化领域数据处理活动，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》《中华人民共和国国家安全法》《中华人民共和国民法典》等法律法规，制定本办法。

第二条【适用范围】在中华人民共和国境内开展的工业和信息化领域数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。

第三条【数据定义】工业和信息化领域数据包括工业数据、电信数据和无线电数据。工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

电信数据是指在电信业务经营活动中产生和收集的数据。

无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据。

工业和信息化领域数据处理者是指对工业和信息化领域数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台（站）使用单位等工业和信息化领域各类主体。

第四条【监管机构】在国家数据安全工作协调机制统筹协调下，工业和信息化部负责督促指导各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方工业和信息化主管部门），各省、自治区、直辖市通信管理局（以下统称地方通信管理局）和各省、自治区、直辖市无线电管理机构（以下统称地方无线电管理机构）开展数据安全监管，对工业和信息化领域数据处理者的数据处理活动和安全保护进行监督管理。

地方工业和信息化主管部门负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。地方通信管理局负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。地方无线电管理机构负责对本地区无线电数据处理者的数据处理活动和安全保护进行监督管理。

工业和信息化部及地方工业和信息化主管部门、通信管理局、无线电管理机构统称为行业（领域）监管部门。

行业（领域）监管部门依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。

第五条【产业发展】行业（领域）监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，发展数据安全产业，提升数据安全保障能力，促进数据的创新应用。

工业和信息化领域数据处理者研究、开发、使用数据新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。

第六条【标准制定】行业（领域）监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业相关标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，合作开展国际标准、国家标准、行业标准、团体标准、企业标准制定。引导工业和信息化领域数据处理者开展数据管理、数据安全贯标达标工作。

第二章 数据分类分级管理

第七条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范，指导开展数据分类分级管理工作，制定行业重要数据和核心数据具体目录并实施动态管理。

地方工业和信息化主管部门、通信管理局、无线电管理

机构组织开展本地区工业和信息化领域数据分类分级管理及重要数据和核心数据识别工作，确定本地区行业（领域）重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。

工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成目录。

第八条【分类分级方法**】**根据行业要求、特点、业务需求、数据来源和用途等因素，工业和信息化领域数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据等。

根据数据遭到篡改、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、组织合法权益等造成的危害程度，工业和信息化领域数据分为一般数据、重要数据和核心数据三级。

工业和信息化领域数据处理者可在此基础上细分数据的类别和级别。

第九条【一般数据**】**危害程度符合下列条件之一的数据为一般数据:

（一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小;

（二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步

和产业生态等影响较小;

（三）其他未纳入重要数据、核心数据目录的数据。

第十条【重要数据**】**危害程度符合下列条件之一的数据为重要数据:

（一）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域;

（二）对工业和信息化领域发展、生产、运行和经济利益等造成严重影响;

（三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大;

（四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响;

（五）经工业和信息化部评估确定的其他重要数据。

第十一条【核心数据**】**危害程度符合下列条件之一的数据为核心数据:

（一）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等与国家

安全相关的重点领域;

（二）对工业和信息化领域及其重要骨干企业、关键信息基础设施、重要资源等造成重大影响;

（三）对工业生产运营、电信网络（含互联网）运行和服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等;

（四）经工业和信息化部评估确定的其他核心数据。

第十二条【重要数据和核心数据目录备案**】**工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门(工业领域)或通信管理局(电信领域）或无线电管理机构（无线电领域）备案。备案内容包括但不限于数据类别、级别、规模、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况，不包括数据内容本身。

地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）应当在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作，备案内容符合要求的，予以备案并发放备案凭证，同时将备案情况报工业和信息化部；不予备案的应当及时反馈备案申请人并说明理由。

重要数据和核心数据的类别或规模变化30％以上的，或

者其它备案内容发生重大变化的，工业和信息化领域数据处理者应当在发生变化的三个月内履行备案变更手续。

第三章 数据全生命周期安全管理

第十三条【主体责任**】**工业和信息化领域数据处理者应当对数据处理活动负安全主体责任，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）建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等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（领域）监管部门开展工作;

（三）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;

（四）根据应对数据安全事件的需要，制定应急预案，并定期进行演练;

（五）定期对从业人员开展数据安全教育和培训;

（六）法律、行政法规等规定的其他措施。

工业和信息化领域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者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人；

（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；

（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。

第十四条【数据收集】工业和信息化领域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。

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人员、设备的管理，并对收集时间、类型、数量、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，工业和信息化领域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。

第十五条【数据存储】工业和信息化领域数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理，定期开展

数据恢复测试。存储核心数据的，还应当实施异地容灾备份。

第十六条【数据使用加工】工业和信息化领域数据处理者利用数据进行自动化决策分析的，应当保证决策分析的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

工业和信息化领域数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。

第十七条【数据传输】工业和信息化领域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。

第十八条【数据提供】工业和信息化领域数据处理者提供数据，应当明确提供的范围、类别、条件、程序等，并与数据获取方签订数据安全协议。提供重要数据和核心数据的，应当对数据获取方数据安全保护能力进行评估或核实，采取必要的安全保护措施。

第十九条【数据公开】工业和信息化领域数据处理者应当在数据公开前分析研判可能对公共利益、国家安全产生的影响，存在重大影响的不得公开。

第二十条【数据销毁】工业和信息化领域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。个人、组织依据法律规定、合同约定等请求销毁的，工业和信息化领域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，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案，不得以任何理由、任何方式对销毁数据进行恢复。

第二十一条【数据出境】工业和信息化领域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和核心数据，法律、行政法规有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

工业和信息化部根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国工业、电信、无线电执法机构关于提供工业和信息化领域数据的请求。非经工业和信息化部批准，工业和信息化领域数据处理者不得向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据。

第二十二条【数据转移】工业和信息化领域数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。涉及重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）

或无线电管理机构（无线电领域）更新备案。

第二十三条【委托处理】工业和信息化领域数据处理者委托他人开展数据处理活动的，应当通过签订合同协议等方式，明确委托方与被委托方的数据安全责任和义务。委托处理重要数据和核心数据的，应当对被委托方的数据安全保护能力、资质进行评估或核实。

除法律、行政法规等另有规定外，未经委托方同意，被委托方不得将数据提供给第三方。

第二十四条【核心数据跨主体处理】跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工业和信息化部。工业和信息化部按照有关规定进行审查。

第二十五条【日志留存】工业和信息化领域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。日志留存时间不少于六个月。

第四章 数据安全监测预警与应急管理

第二十六条【监测预警机制】工业和信息化部建立数据安全风险监测机制，组织制定数据安全监测预警接口和标准，统筹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。

地方工业和信息化主管部门、通信管理局和无线电管理机构建设本地区数据安全监测预警机制，组织开展本地区工业、电信行业和无线电数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和信息化领域数据处理者及时采取应对措施。

工业和信息化领域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。

第二十七条【信息上报和共享】工业和信息化部建立数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报数据安全风险信息，鼓励安全服务机构、行业组织、科研机构等开展数据安全风险信息上报和共享。

地方工业和信息化主管部门、通信管理局和无线电管理机构汇总分析本地区工业、电信行业和无线电数据安全风险，及时将可能造成重大及以上安全事件的风险上报工业和信息化部。

工业和信息化领域数据处理者应当及时将可能造成较大及以上安全事件的风险向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。

第二十八条【应急处置】工业和信息化部制定工业和信息化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。

地方工业和信息化主管部门、通信管理局和无线电管理机构组织开展本地区工业、电信行业和无线电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，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。

工业和信息化领域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，应当第一时间向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。事件处置完成后应当在规定期限内形成总结报告，每年向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告数据安全事件处置情况。

工业和信息化领域数据处理者对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。

第二十九条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，地方工业和信息化主管部门、通信管理局、无线电管理机构建立本地区工业、电信行业和无线电数据安全违法行为投诉举报机制或渠道，依法接收、处理投诉举报，根据

工作需要开展执法调查。鼓励工业和信息化领域数据处理者建立用户投诉处理机制。

第五章 数据安全检测、认证、评估管理

第三十条【安全检测与认证】工业和信息化部鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作。

第三十一条【安全评估】工业和信息化部制定行业数据安全评估机构管理制度，开展评估机构管理工作。制定行业数据安全评估规范，指导评估机构开展数据安全风险评估、合规评估、能力评估、出境评估等工作。

地方工业和信息化主管部门、通信管理局和无线电管理机构负责组织开展本地区工业、电信行业和无线电数据安全评估工作。

工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年至少开展一次安全评估，及时整改风险问题，并向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报送评估报告。

第六章 监督检查

第三十二条【监督检查和协助义务】行业（领域）监管部门对工业和信息化领域数据处理者落实本办法要求的情况进行监督检查。

工业和信息化领域数据处理者应当对行业（领域）监管部门监督检查予以配合。

第三十三条【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，开展数据安全审查相关工作。

第三十四条【保密要求】行业（领域）监管部门及其委托的数据安全评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

第七章 法律责任

第三十五条【约谈整改】行业（领域）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工业和信息化领域数据处理者进行约谈，并要求采取措施进行整改，消除隐患。

第三十六条【法律责任】有违反本办法规定行为的，由行业（领域）监管部门依照相关法律法规，根据情节严重程度给予没收违法所得、罚款、暂停业务、停业整顿、吊销业务许可证等行政处罚；构成犯罪的，依法追究刑事责任。

第八章 附则

第三十七条【个人信息保护】开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第三十八条【其他规定参照】涉及军事、国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。

第三十九条【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。

第四十条【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。

第四十一条【施行日期】本办法自 2022 年 月 日起施行。