附件1

工业和信息化领域数据安全管理办法（试行）

（征求意见稿）

第一章 总则

第一条【目的依据】为了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《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国网络安全法》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电信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】工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计、生产制造、经营管理、运维服务、平台运营、应用服务等过程中收集和产生的数据。

电信数据是指在电信业务经营活动中收集和产生的数据。

工业和电信数据处理者是指对工业、电信数据进行收

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和取得电信业务经营许可证的电信业务经营者等工业和信息化领域各类主体。

第四条【监管机构】工业和信息化部负责对工业和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。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）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。各省、自治区、直辖市通信管理局（以下统称地方通信管理局）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。

工业和信息化部及地方工业和信息化主管部门、通信管理局统称为行业监管部门。

第五条【产业发展】行业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，壮大数据安全产业，提升数据安全保障能力，促进数据的创新应用。

工业和电信数据处理者研发提供数据开发利用新技术、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，开展国际标准、国家标准、团体标准、企业标准制定。引导工业和电信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【分类分级方法】工业和电信数据处理者应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单。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、个人信息等。

工业和信息化部按照国家有关规定，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，将工业和电信数据分为一般数据、重要数据和核心数据三级。

第八条【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）恢复数据或消除负面影响所需付出的代价小;

（四）其他未纳入重要数据、核心数据目录的数据。

第九条【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、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、人工智能等重点领域国家安全相关数据的安全;

（二）对工业、电信行业发展、生产、运行和经济利益等造成影响;

（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）恢复数据或消除负面影响所需付出的代价大;

（六）经行业监管部门评估确定的其他重要数据。

第十条【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、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、人工智能等重点领域国家

安全相关数据的安全;

（二）对工业、电信行业及其重要骨干企业、关键信息基础设施、重要资源等造成严重影响;

（三）对工业生产运营、电信和互联网运行和服务等造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、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。

第十一条【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及数据分级防护等制度规范，形成行业重要数据和核心数据具体目录并实施动态管理，指导开展数据分类分级防护工作。

地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护及重要数据和核心数据识别认定工作，形成本地区行业重要数据和核心数据具体目录并上报工业和信息化部。

工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。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。

第十二条【重要数据和核心数据备案管理】工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。

地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。

工业和电信数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。

第三章 数据全生命周期安全管理

第十三条【主体责任】工业和电信数据处理者应当对数据处理活动负安全主体责任，根据数据的类型、数量、安全级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等，采取必要措施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）明确数据安全管理的主要负责人和责任部门，统筹负责数据处理活动的安全监督管理;

（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）制定数据安全事件应急预案，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、行政法规规定的其他措施。

第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。

第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。

第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。

第十七条【数据收集】工业和电信数据处理者收集数据

应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。

数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。

通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

第十八条【数据存储】工业和电信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。存储重要数据的，还应当采用校验技术、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。存储核心数据的，还应当实施异地容灾备份。

第十九条【数据使用加工】工业和电信数据处理者未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。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。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。

工业和电信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。

第二十条【数据传输】工业和电信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。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。

第二十一条【数据提供】工业和电信数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。

工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。

第二十二条【数据公开】工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。

第二十三条【数据销毁】工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等

要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。

符合以下情况之一的，工业和电信数据处理者应当销毁相应数据:

（一）因业务约定，需要销毁的;

（二）个人依据其合法权益请求销毁的;

（三）组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。

第二十四条【数据出境】工业和电信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，应当依照法律、行政法规要求在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。核心数据不得出境。

第二十五条【数据承接】工业和电信数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据承接方案，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，应当及时向所在地工业和信息化主管部门或通信管理局备案。

作为数据承接方的工业和电信数据处理者，应当及时向所在地工业和信息化主管部门或通信管理局备案，承担数据安全责任和保护义务，不得违反国家有关规定及原数据处理者与用户的约定。

重要数据和核心数据没有承接方且符合销毁条件的，工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的，工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局，将数据移交至行业监管部门指定的机构进行保存。

第二十六条【委托处理】工业和电信数据处理者委托他人开展数据处理活动的，应当对被委托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，并通过合同约束、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对被委托方进行安全评估。

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

第二十七条【安全审计】工业和电信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，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。

第四章 数据安全监测预警与应急管理

第二十八条【监测预警机制】工业和信息化部统筹建立

工业和信息化领域数据安全风险监测机制，建设数据安全监测预警平台，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。

地方工业和信息化主管部门、通信管理局建设数据安全监测预警平台，组织开展本地区工业、电信行业数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和电信数据处理者及时采取应对措施。

工业和电信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。

第二十九条【信息上报和共享】工业和信息化部统一汇集、分析、通报工业和信息化领域数据安全风险信息，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和事件等相关信息上报和共享。

地方工业和信息化主管部门、通信管理局汇总分析本地区工业、电信行业数据安全风险和事件信息，及时将涉及重要数据和核心数据的安全风险上报工业和信息化部。

工业和电信数据处理者应当及时将自身数据安全风险情况向所在地工业和信息化主管部门或通信管理局报告。

第三十条【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、通信管理局组织开展本地区工业、电信行业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。

工业和电信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，应当第一时间向所在地工业和信息化主管部门或通信管理局报告。事件处置完成后应当在规定期限内形成总结报告，每年向所在地工业和信息化主管部门或通信管理局报告数据安全事件处置情况。

工业和电信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。

第三十一条【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，及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处理者下发相关投诉举报信息。地方工业和信息化主管部门、通信管理局组织工业和电信数据处理者对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。

工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到

投诉之日起15个工作日内答复投诉人。

第五章 数据安全检测、评估与认证管理

第三十二条【安全能力认证】工业和信息化部建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。

第三十三条【安全评估】工业和信息化部制定工业和信息化领域数据安全评估规范，指导检测评估机构开展数据安全风险评估、合规评估等工作。地方工业和信息化主管部门、通信管理局负责组织开展本地区工业、电信行业数据安全评估。

工业和电信数据处理者应当依据数据安全评估规范，开展数据安全评估及整改。

（一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改；

（二）对于重要数据和核心数据，应当至少每年自行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。

第六章 监督检查

第三十四条【监督检查和协助义务】工业和信息化部组

织制定数据安全监测接口标准。行业监管部门对工业和电信数据处理者落实本规定要求的情况进行监督检查。工业和电信数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。

第三十五条【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，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。

第三十六条【保密要求】行业监管部门及其委托的数据安全检测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、出售或者非法向他人提供。

第三十七条【约谈整改】行业监管部门在履行数据安全监督管理职责中，对未按要求进行重要数据和核心数据备案，或者发现数据处理活动存在重大安全风险或发生安全事件的，可以按照规定权限和程序对工业和电信数据处理者的法定代表人或者主要负责人进行约谈，并要求采取措施进行整改，消除隐患。

第七章 法律责任

第三十八条【信用机制】行业监管部门应当将工业和电信数据处理者落实数据安全管理责任情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。

第三十九条【法律责任】对于违反本办法的，由行业监管部门依照《数据安全法》《网络安全法》等法律和相关行政法规，根据情节严重程度给予公开曝光、没收违法所得、罚款、暂停业务、停业整顿、关闭网站、吊销业务许可证或吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。

第八章 附则

第四十条【涉密排除】涉及国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。

第四十一条【军事数据排除】涉及军事的数据处理活动，按照国家有关规定执行。

第四十二条【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。

第四十三条【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。

第四十四条【施行日期】本规定自 年 月 日起施行。