佳 木 斯 市 数 据 局
中共佳木斯市委网络安全和信息化委员会办公室
中共佳木斯市委保密和机要局 文件
佳 木 斯 市 公 安 局
佳木斯市营商环境建设监督局

佳数联规〔2025〕1号

关于印发《佳木斯市公共数据安全管理办法（试行）》的通知

各县（市）区人民政府，市直、中省直各有关单位，相关企业：

为规范和加强佳木斯市公共数据安全管理，根据《中华人民共和国国家安全法》《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规和有关规定，市数据局、市委网信办、市委保密和机要局、市公安局、市营商环境建设监督局共同制定了《佳木斯市公共数据安全管理办法（试行）》。现印发

给你们，请遵照执行。

佳木斯市数据局

中共佳木斯市委网络安全和信息化委员会办公室

中共佳木斯市委保密和机要局

佳木斯市公安局

佳木斯市营商环境建设监督局

2025年1月17日

佳木斯市公共数据安全管理办法（试行）

第一章　总　则

第一条　为规范佳木斯市公共数据处理活动，加强公共数据安全管理，保障数据安全，促进数据开发利用，保障全市数字化系统安全稳定运行，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》《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《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　在佳木斯市行政区划范围内开展的公共数据处理活动及其安全监管，应当遵守相关法律、行政法规、地方性法规、地方政府规章和本办法的要求。

第三条　本办法中所指的数据皆为公共数据。

公共数据，是指国家机关和法律、法规授权的具有管理公共事务职能的组织以及供水、供电、供气、供热、通讯、公共交通等公共服务运营单位（以下统称公共管理和服务机构）在依法履职或者提供公共管理和服务过程中收集、产生的，以一定形式记录、保存的各类数据及其衍生数据，包含政务、公益事业单位数据和公用企业数据。

第四条 本办法中提到的数据处理者，遵照国家、省级相关法律法规、标准规范等进行确定。数据处理活动包括数据的收集、存储、使用、加工、传输、提供、公开等。

第五条 在佳木斯市数据安全工作协调机制下，数据管理部门负责督促指导各行业主管部门开展数据安全监管，对公共数据处理活动及安全保护进行监督管理。各行业主管部门分别负责对本地区本行业单位的数据处理活动和安全保护进行监督管理。同时行业主管部门有义务按照有关法律及行政法规，配合数据、网信、公安、保密等有关部门开展数据安全监管相关工作。

第六条 数据管理部门负责推进本地区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度的修订及推广应用工作。

第二章 数据安全分类分级管理

第七条 数据管理部门依据国家数据局、省数据局、行业主管部门等相关政策要求，指导佳木斯市全域数据分类分级、重要数据和核心数据识别认定、数据分级防护等工作，制定本市重要数据和核心数据目录并实施动态管理。

佳木斯市各行业主管部门分别组织开展数据分类分级管理及重要数据和核心数据识别工作，确定本地区本行业重要数据和核心数据具体目录并同步报数据管理部门，报送内容包括但不限于

数据来源、类别、级别、规模、载体、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，目录发生变化的，应当及时上报更新。

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本单位的具体目录。

第八条 依照国家相关标准对本办法中所指数据进行分类分级。数据处理者根据数据的属性及特征，将其按一定原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序。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，数据分为一般数据、重要数据和核心数据三级。

危害程度符合下列条件之一的为一般数据。

（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。

危害程度符合下列条件之一的为重要数据。

（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）对城市发展、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）恢复数据或消除负面影响所需付出的代价大；

（六）经行业主管部门评估确定的其他重要数据。

危害程度符合下列条件之一的为核心数据。

（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）对城市重要骨干企业、关键信息基础设施、重要资源等造成重大影响；

（三）对各企业生产运营、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）经行业主管部门评估确定的其他核心数据。

第三章　数据全生命周期安全管理

第九条　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）建设数据安全基础防护能力，包括：国产密码技术的密码基础设施及数据动静态脱敏设施，以提供数据在存储、使用、传输、提供、公开等环节的数据安全保护；

（三）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，协助行业主管部门开展工作；

（四）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；

（五）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；

（六）定期对从业人员开展数据安全教育和培训；

（七）法律、行政法规等规定的其他措施。

重要数据和核心数据的处理者，还应当：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，分管数据安全的领导是直接责任人；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；建立内部登记、审批等工作机制，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。

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，并记录收集来源、时间、类型、数量、频度、流向等。

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。

第十一条　数据处理者应当按照法律、行政法规规定和用户约定的方式、期限进行数据存储。存储重要数据和核心数据的，应当按照国家相关标准采用国产商用密码技术安全存储，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。

第十二条　数据处理者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。

第十三条　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，须按照国家相关标准采用国产商用密码技术进行传输过程的数据安全保护。

第十四条　数据处理者对外提供数据，应当明确提供的范围、类别、条件、程序等。其中重要数据和核心数据应委托第三方专业机构进行数据安全评估，出具评估报告交市级数据管理部门审核通过后，方可提供。对提供重要数据和核心数据的，数据处理者还应与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，并采取数据脱敏等安全保护措施。

第十五条　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，存在重大影响的不得公开。

第十六条　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。数据处理者销毁重要数据和核心数据后，不得以任何理由、任何方式对销毁数据进行恢复，引起本单位重要和核心数据目录内容发生变化的，应当立即向行业主管部门进行报备。

第十七条　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。

第十八条　数据处理者因机构改革、撤销，以及兼并、重

组、破产等原因需要转移数据的，应明确数据转移方案，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目录内容发生变化的，应当立即向行业主管部门报备。

第十九条 数据处理者委托他人开展数据处理活动的情况，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。委托处理重要数据和核心数据的，应当对受托方的数据安全保护能力、资质进行核验。

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

第二十条 跨主体提供、转移、委托处理核心数据的情况，数据处理者应当评估安全风险，采取必要的安全保护措施，并报本地区行业主管部门审查。

第二十一条 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。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

第二十二条 按照“谁管业务、谁管业务数据、谁管数据安全”的原则，实行数据安全监测预警与应急管理，保障数据全生命周期安全。

第二十三条 数据管理部门建立本地区数据安全风险监测预警机制，统筹开展数据安全监测预警，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。

第二十四条 各行业主管部门汇总分析本地区本行业数据安全风险，及时上报。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本地区行业主管部门报告。

第二十五条 数据管理部门制定本地区数据安全事件应急预案，组织协调本地区重要数据和核心数据安全事件应急处置工作。

佳木斯市各行业主管部门分别组织开展本地区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，应当立即报告市数据管理部门，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，应当按照应急预案内容，及时开展应急处置，涉及重要数据和核心数据的安全事件，第一时间向本地区行业主管部门报告，事件处置完成后在规定期限内形成总结报告，每年向本地区行业主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　数据安全评估管理

第二十六条　数据管理部门牵头负责组织开展本地区数据安全评估工作。

第二十七条　全市拟立项涉公共数据的数字化项目，应在立项前向市级数据管理部门提交数据安全建设方案，未提供方案的，由数据管理部门出具书面建议，视情况重新开展立项审核。

已立项项目应由立项单位在项目验收环节组织有资质的专业机构对项目所涉及的数据开展数据安全风险评估，并由该机构出具数据安全风险评估报告报市级数据管理部门。

已建设完成运行的信息化项目，每年应对项目所涉及的数据开展至少一次数据安全风险评估，出具数据安全风险评估报告报市级数据管理部门。

重要数据处理者每年开展至少一次数据安全风险评估。

第六章　监督检查

第二十八条　数据管理部门统筹各行业主管部门对本地、本部门、本行业数据处理者落实本办法要求的情况进行监督检查。各行业主管部门每年至少对本部门、本行业开展一次数据安全专项检查，评估数据安全风险隐患。数据处理者应当对行业主管部门监督检查予以配合。

第二十九条　数据管理部门会同网信、公安、保密、营商等

部门在佳木斯市数据安全工作协调机制指导下，开展全市数据安全监督检查相关工作。

第七章　法律责任

第三十条　各级行业主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相关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。

第三十一条　开展数据处理活动的组织、个人不履行本管理办法规定的数据安全保护义务的，由市级数据管理部门会同有关行政执法部门参照《中华人民共和国数据安全法》等相关法律法规给予相应处罚。

第八章　附　则

第三十二条　开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第三十三条　按照本办法第十四条相关规定，数据处理者不得自行开展公共数据授权运营。

第三十四条　涉及军事、国家秘密信息等数据的处理活动，按照国家有关规定执行。

第三十五条　本办法生效期内相关条款如与上级有关规定冲

突，以上级规定为准。

第三十六条　本办法自2025年2月1日起施行，有效期1年。

第三十七条　本办法最终解释权归佳木斯市数据局所有。

抄送：市委国安办

佳木斯市数据局综合规划科　　2025年1月17日印发