HDFS01—2025—0002

海东市人民政府办公室文件

东政办〔2025〕24号

海东市人民政府办公室
关于印发海东市数据安全管理
办法（暂行）的通知

各县区人民政府，海东工业园区管委会，市政府各部门：

《海东市数据安全管理办法（暂行）》已经市政府第65次常务会议审议通过，现印发给你们，请结合工作实际，抓好贯彻落实。

2025年3月31日

海东市数据安全管理办法（暂行）

第一章　总 则

第一条 为贯彻国家总体安全观，规范全市资源资产数据安全管理，建立数据安全协调机制，健全数据安全保障体系，预防数据安全事件发生，保护各类主体包括个人、组织的合法权益，依法促进数据资源开放、开发利用，根据《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》《中华人民共和国保守国家秘密法》等有关规定，结合海东实际，制定本办法。

第二条 本办法适用于海东市行政区域内的非涉密数据安全管理工作。涉及国家秘密的数据，按照国家保密相关规定管理和使用。

第三条 数据安全采取积极防御、综合防范，统一协调、统筹规划，分级管理、分工负责的方针，坚持保障数据安全与促进信息化、数字化发展相协调，管理与技术统筹兼顾，遵循谁收集谁负责、谁持有谁负责、谁管理谁负责、谁开放谁负责、谁使用谁负责、谁运维谁负责的基本原则，推进数据安全和信息化、数字化工作同步规划、同步建设、同步实施、同步发展。

第二章　管理职责分工

第四条 市数据局作为全市数据主管部门，履行下列职责：

（一）依照国家、省、市、行业、领域数据安全法律、法

规、规章和标准，规划全市数字经济、数字政府、数字社会发展、统筹、组织、协调、指导和监督全市数据要素安全管理工作，组织建立数据要素管理制度，指导推动数据资源在各领域的应用建设，指导各县区数据主管部门开展数据安全管理工作；

（二）指导监督相关部门执行数据安全相关标准和技术规范，健全完善适应于大数据环境下的数据分类分级安全管理制度，制定适合全市数字经济新产业、新业态、新应用模式的数据分类分级规则，为数据安全管理和安全资源配置提供指导；

（三）统筹协调机关企事业单位信息资源数据共享审批、授权运营，制定机关企事业单位信息资源数据共享审批、授权运营规则，组织建设和完善全市数据安全保障基础设施，引进数据安全专家队伍，利用科学的数据安全管理和技术手段，为数据的全生命周期管控提供支撑；

（四）负责组织做好数据安全领域相关的法律标准解读、风险评估、安全培训等工作；

（五）会同网信、公安、工信、保密、电子政务等有关部门，按照各自职责分工对各单位各部门进行数据安全检查，对发现的问题及隐患提出指导建议；

（六）法律、法规、标准、规章规定的其他职责。

第五条 市政务服务监管局作为承担全市政务服务的工作部门，协同市数据局、市政府办公室推进数据依法开放、共享工作。

第六条 市政府办公室作为统筹电子政务外网、政务专网建设的工作部门，协同市数据局、市政务服务监管局、市公安局、市委网信办、市委机要和保密局、行业监管部门、各相关部门推进数据依法开放、共享工作。

第七条 各县区数据主管部门在市数据主管部门的指导下负责本行政区域内数据安全管理工作，会同本级网信、公安等部门开展数据安全检查，建立数据安全风险监测预警、信息通报和应急处置机制等。

第八条 公共管理和服务机构作为公共数据管理的责任主体，在市数据主管部门的指导下申请采购企业数据和个人数据。

第九条 市、县区网信部门在市数据主管部门的指导下，管理和监督互联网信息内容，保障网络信息安全，负责统筹本级企事业单位网络及数据安全相关规划、宣传等工作。

市、各县区公安机关在市数据主管部门的指导下，在各自职责范围内承担本级各企事业单位网络安全及数据安法执法、等级保护备案、监督、检查、指导等职责。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

市、县区密码管理部门负责管理本行政区域的商用密码应用安全性评估工作。涉及商用密码工作的单位在其职责范围内负责指导、监督本机关、本单位或者本系统的商用密码应用安

全性评估工作。

市、县区保密部门制定本级管辖区内的保密工作计划并组织实施，履行保密行政管理职能，负责有关保密法规、规章的宣传、指导、监督、检查，参与对机关、单位的保密检查。

工业、电信、交通、金融、自然资源、卫健、教育、科技、政务服务、电子政务等主管部门在市数据主管部门的指导下承担本行业、本领域数据安全监管职责。

各单位信息归口部门在市数据主管部门的指导下负责本单位的业务数据安全工作，履行下列职责:

（一）执行国家、省、市数据安全法律、法规、规章和标准，履行数据安全保护义务，对工作中收集和产生的数据及数据安全负责，指定数据安全管理人员，落实数据安全责任制;

（二）制定本单位数据安全计划，实施数据安全防护技术措施，开展数据安全风险评估，有效应对数据安全事件，防范违法犯罪活动;

（三）参加数据安全教育培训，接受有关部门监管和社会监督;

（四）承担其他数据安全相关工作。

第十条 为统一管理全市信息化项目规划、申报审批、技术审查，以及项目建设管理、验收评价、运营维护等阶段的数据安全建设工作，市数据局协同市委国家安全委员会办公室、市委网信办、市委机要和保密局、市发展改革委、市公安局、市

工业信息化局，组成数据安全工作协调机制，办公室设立在市数据局，并按照分工履行下列职责:

市数据局负责制定统一信息化技术架构、数据架构、应用架构；负责跨行业、跨部门的资源整合、互联互通和重要信息资源的开发、利用、共享；负责市本级、各县区政府、各园区管委会信息化项目技术审查和统一规划指导。

市委网信办协调市审计局负责信息化项目的数据安全审查，参与技术评审，确保项目在规划、设计、实施及运营各阶段均符合国家和地方的网络安全法律法规及相关标准，保障信息化项目的健康发展和安全稳定运行。

市委机要和保密局负责指导信息化项目的密码安全方案设计并协助开展评审，保障信息传输、存储和处理过程中的数据安全和隐私保护，支持信息化建设的数据安全需求。

市发展改革委负责政务信息化项目规划、审批、备案、监管职责，市政府办公室负责信息化项目技术审查。

市公安局负责监督和管理信息化项目网络等级保护工作，确保重要信息系统达到相应的数据安全保护水平，为信息化项目的建设和运行提供安全保障。

市工业信息化局负责参与信息化项目的评审和技术指导，确保项目符合产业发展方向和数据安全技术标准。

市国安局负责在信息化项目中，关注涉及国家安全的信息系统和数据的安全，防止境外势力的渗透、破坏、窃密等活动，

确保国家秘密和重要敏感信息的安全，参与相关项目的数据安全评估和审查，保障国家利益不受损害。

各信息化项目建设单位负责项目的方案编制、申请报批、建设实施、进度跟踪、质量保证、运行维护及应用推广。在项目竣工验收阶段，建设单位应向市数据局提交安全风险评估报告、代码审计报告，经市数据局审核通过后方可正式上线。信息化项目中非涉密但涉及敏感信息的政务数据信息，经过脱敏、清洗、加工后，可根据使用条件和适用范围无条件开放或者有条件开放。

数据安全工作协调办公室全面统筹和加强全市信息化项目的全生命周期数据安全管理，负责规划指导、监督审查信息化项目的申报审批、技术审查、建设管理、验收评估及运营维护等各环节中的数据安全管理要求落实情况，确保信息安全合规，防范数据泄露风险，促进信息技术健康发展。

第十一条 其他部门职责依照《海东市数据要素管理办法（暂行）》第二章职责分工相关要求执行。

第三章 数据安全应急监测管理

第十二条 根据问题事件影响对象的重要程度、业务损失的严重程度和社会危害的严重程度三个要素对问题事件划分四个等级。通过分别评定业务损失的严重程度和社会危害的严重程度，确定数据安全事件级别。（详见附录 表 2 数据安全事件级别与业务损失的严重程度的关系，表 3 数据安全事件级别与社

会危害的严重程度关系）

第十三条 数据主管部门应该组织开展数据安全风险评估，加强对数据要素各项活动的风险监测，建立数据安全应急处置机制，及时发现问题并采取防护和补救措施。

第十四条 数据主管部门按照国家相关标准和流程，组织建立数据安全风险监测机制，建立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。各县区数据主管部门组织建立数据安全风险监测预警机制，划分数据安全风险和事件等级，组织建设数据监测预警技术手段。

各县区数据主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。

发生数据安全事件，市公安机关应当会同市网信部门依照相关应急预案，采取应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第十五条 数据主管部门组织建立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。各县区数据主管部门组织建设本级数据安全风险信息通报机制。

行业监管部门分别汇总分析本地区各行业数据安全风险，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市数据局报告。

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。

第十六条 数据主管部门牵头制定数据安全事件应急预案，会同公安机关、网信部门和密码管理部门组织协调重要数据和核心数据安全事件应急处置工作。各县区数据主管部门组织建设本级数据安全事件应急预案，会同相关部门组织协调重要数据和核心数据安全事件应急处置工作。

行业监管部门分别组织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，应当立即报市数据局，并及时报告事件发展和处置情况。

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。在数据安全事件发生后，应当按照应急预案，第一时间向行业监管部门、属地公安部门、网信部门报告，及时开展应急处置，涉及重要数据和核心数据的安全事件，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。

第十七条 各部门应当根据实际需要与网信、公安、当地运

营商、电网等部门建立应急协调机制，及时处理由网络中断、电力供应和非法攻击行为等引发的数据安全事件。

第十八条 数据出现下列情形之一时，各部门应当立即采取补救措施，并报送同级网信、公安、保密等部门：

（一）发现重大网络安全隐患、漏洞或基础网络、重要系统受到外部攻击遭到破坏的；

（二）发生重大数据安全事件的；

（三）公民、法人信息或重要业务数据泄露、毁损、丢失，造成重大影响或经济损失的；

（四）行政机关及事业单位等网站数据被篡改；

（五）国家、省、市数据安全主管部门通报的事件；

（六）其他需要调查的。

第四章 数据分类分级管理

第十九条 数据安全工作协调机制办公室组织制定数据分类分级、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。

第二十条 市直有关部门在市数据安全工作协调机制的指导下，按照数据分类分级标准规范，分别组织开展本地区本行业数据分类分级管理及重要数据和核心数据识别工作，结合工作需要编制相应领域数据安全标准规范，指导开展行业数据分类分级工作。编制本行业地区重要数据和核心数据目录，并上报协调机制办公室实施动态管理，目录发生变化的，应及时上

报更新。

第二十一条 **数据监管部门**根据行业特点和业务应用，通过对数据重要性、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。

第二十二条 数据处理者应当定期按照数据分类分级标准规范，根据监管要求梳理填报重要数据和核心数据目录。制定数据全生命周期安全防护要求和操作规程，配套建设差异化的数据安全风险监测技术手段，加强数据安全风险的分析、研判、预警和处置能力。

第五章 数据安全审查管理

第二十三条 数据提供者对所提供的各级各类数据在产生、存储、使用、传播、销毁等全生命周期中的安全控制措施及行为等进行数据安全审查。

第二十四条 各单位应当明确采集数据的目的和用途，确保数据采集的合法性、正当性、必要性和业务关联性。对数据采集的环境、设施和技术采取必要的管控措施，确保数据的完整性、一致性和真实性。

第二十五条 数据责任主体应当建立信息系统和数据资产管理体系，实行资产登记，编制资产清单，明确资产管理责任

部门与人员，按照监管数据安全工作规则定期开展自查,并保留检查记录。发现监管数据安全缺陷、漏洞等风险时,应立即采取补救措施。

第二十六条 数据主管部门牵头建立数据安全审查制度，在数据提供者自审查的基础上，对影响或者可能影响国家安全的重要和核心数据处理活动进行数据安全审查。各县区数据主管部门和行业监管部门遵循市数据安全审查制度履行各县区及行业数据安全审查职责。

第二十七条 在审查过程中，审查人员应依照数据相应级别的保密要求对接触到的敏感数据进行严格保密，尤其在安全漏洞修补之前，严禁泄露。

第六章 全流程数据安全管理

第二十八条 数据处理者应当对数据处理活动安全负主体责任，数据同时存在多个处理者的，各数据处理者承担相应的安全责任。数据处理者发生变更时，应同步完成数据安全保护责任的主体变更，保证权责同步交给新的数据处理者。

第二十九条 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。

第三十条 各县区、各单位应当建立数据安全管理制度，履行以下职责:

（一）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）根据数据安全管理工作的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，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职责。

重要数据和核心数据处理者，还应当履行以下职责：

（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，对关键岗位人员进行背景审查，并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，提交市公安机关进行安全背景审查；

（三）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；

（四）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；

第三十一条 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，对数据采集的环境、设施和技术采取必要的管控措施，确保数据的完整性、一致性和真实性，保证数据在采集过程中不被泄露；

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。

第三十二条 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，须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，须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。

第三十三条 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。

第三十四条 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。

第三十五条 数据处理者应当按照有关规定安全有序提供数据，制定数据共享、交换、发布管理制度，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，还应当采取其他必要的安全保护措施。

第三十六条 各有关主管部门应当遵守公正、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。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。

第三十七条 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、数据管理部门申请审核后向协调机制办公室报告数据销毁方案。引起重要数据和核心数据目录变化的，应及时向行业监管部门、数据管理部门申请审核后向协调机制办公室报备，不得以任何理由、任何方式对销毁数据进行恢复。

第三十八条 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，数据出境需合法依规，确保安全。

第三十九条 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。

第四十条 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。

第四十一条 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，并采用适当的商用密码技术保护日志的完整性，确保日志留存时间满足事件溯源需要，日志记录留存时间不少于六个月。

第七章 关键数据基础设施安全管理

第四十二条 市公安局牵头指导落实对关键数据基础设施保护制度，强化和落实关键数据基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键数据基础设施安全。采取必要措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，依法保护关键数据基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键数据基础设施安全的违法犯罪活动。

第四十三条 关键信息基础设施运营者应当依照本办法和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第四十四条 关键信息基础设施运营者应当建立健全关键

信息基础设施安全保护制度和责任制。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第四十五条 关键信息基础设施运营者应当设置专门安全管理机构，由公安机关牵头，协同密码机关对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

第八章　数据开放共享安全管理

第四十六条 数据主管部门会同相关部门对政务数据、企事业单位信息资源数据和社会数据统筹管理。

第四十七条 按照数据共享属性，政务数据分为无条件共享、有条件共享、不予共享等三种类型。

可提供给所有政务部门共享使用的政务信息数据属于无条件共享类。

可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用的政务信息数据属于有条件共享类。

不宜提供给其他政务部门共享使用的政务信息数据属于不予共享类。

第四十八条 企事业单位信息资源数据根据数据安全要求、个人信息保护要求和应用要求等因素分为无条件开放、有条件开放和非开放三种类型。（详见附录）

第四十九条 充分发挥政务数据共享协调机制作用，提升数据共享统筹协调力度和服务管理水平。全市标准统一、动态管理的政务数据目录，实行“一数一源一仓一标准”，实现数据资源清单化管理。充分发挥大数据统一纳管平台的共享枢纽作用，实现政府信息系统与党委、人大、政协、法院、检察院等信息系统互联互通和数据按需共享。有序推进市属部门垂直管理业务系统与地方数据平台、业务系统数据双向共享。以政务模型、应用场景为牵引，建立健全政务数据供需对接机制，推动数据精准高效共享，大力提升数据共享的实效性。

第五十条 数据主管部门应会同相关部门建立企事业单位信息资源数据授权运营机制，制定企事业单位信息资源数据授权运营管理办法，各级数据管理机构应当根据企事业单位信息资源数据授权运营管理办法对授权运营单位实施日常监督管理。

第五十一条 公共管理和服务机构之间共享企事业单位信息资源数据，应当以共享为原则，不共享为例外。企事业单位信息资源数据应当通过大数据统一纳管平台进行共享。

公共管理和服务机构应当根据履职需要，提出数据需求清单；根据法定职责，明确本单位可以共享的数据责任清单；对法律、法规明确规定不能共享的数据，经市数据局审核后，列入负面清单。

数据主管部门牵头建立以共享需求清单、责任清单和负面

清单为基础的信息资源数据共享机制。

公共管理和服务机构提出共享需求的，应当明确应用场景，并承诺其真实性、合规性、安全性。对未列入负面清单的企事业单位信息资源数据，可以直接共享，但不得超出依法履行职责的必要范围。对未列入企事业单位信息资源数据目录的企事业单位信息资源数据，市级责任部门应当在收到共享需求之日起十五个工作日内进行确认后编入企事业单位信息资源数据目录并提供共享。

公共管理和服务机构超出依法履行职责的必要范围，通过大数据统一纳管平台获取其他机构共享数据的，市数据局应当在发现后应要求其停止获取超出必要范围的数据。

第五十二条 公共管理和服务机构向自然人、法人和非法人组织提供服务时，需要使用其他部门数据的，应当使用大数据统一纳管平台提供的最新数据。

公共管理和服务机构应当建立共享数据管理机制，通过共享获取的企事业单位信息资源数据，应当用于本单位依法履行职责的需要，不得以任何形式提供给第三方，也不得用于其他任何目的，加强对数据流向的追溯。

第五十三条 市数据局以需求导向、分级分类、公平公开、安全可控、统一标准、便捷高效为原则，推动企事业单位信息资源数据面向社会开放，并持续扩大企事业单位信息资源数据开放范围。

第五十四条 数据主管部门协同行业监管部门、地方管理部门积极推进城市人、地、事、物、情、组织等多维度数据融通，支撑公共卫生、交通管理、公共安全、生态环境、基层治理、体育赛事等各领域场景应用，实现态势实时感知、风险智能研判、及时协同处置。支撑城市发展科学决策，支持利用城市时空基础、资源调查、规划管控、工程建设项目、物联网感知等数据，助力城市规划、建设、管理、服务等策略精细化、智能化。推进公共服务普惠化，深化公共数据的共享应用，深入推动就业、社保、健康、卫生、医疗、救助、养老、助残、托育等服务“指尖办”“网上办”“就近办”。加强区域协同治理，推动城市群数据打通和业务协同，实现经营主体注册登记、异地就医结算、养老保险互转等服务事项跨城通办。

第五十五条 数据主管部门会同有关部门，依法依规组织开展企事业单位信息资源数据开放和开发利用的创新试点，鼓励自然人、法人和非法人组织对企事业单位信息资源数据进行深度加工和增值使用。

第九章　数据要素开发共享安全管理

第五十六条 市数据局牵头组建全市统一的数据要素开发、交易公共服务平台，支持数据资源开发和应用，发挥海量数据和丰富应用场景优势，牵头打造安全可信流通环境，深化数据空间、隐私计算、联邦学习、区块链、数据沙箱等技术应用，

探索建设重点行业和领域数据流通平台，增强数据利用可信、可控、可计量能力，促进数据合规高效流通使用，鼓励和引导全社会参与经济、生活、治理等领域全面数字化转型，提升城市软实力。

第五十七条 数据要素交易应当遵循自愿、平等、公平和诚实守信原则，遵守法律法规和商业道德，履行数据安全保护、个人信息保护、知识产权保护等方面的义务。

第五十八条 数据要素交易应遵循市政府授权制度，数据交易服务机构应当建立规范透明、安全可控、可追溯的数据交易服务环境，制定交易服务流程、内部管理制度以及机构自律规则，采取有效措施保护个人隐私、个人信息、商业秘密、保密商务信息等数据。

数据要素交易坚持“宽进严管”原则，在规范市场安全监管和秩序规范的基础上促进数据共享开放，推动提高数据流通效率，加强对数据供给、流通、应用全过程中的一体化安全保障，构建数据来源可确认、使用范围可界定、流通过程可追溯，构建符合数据交易安全合规的管理制度。

在数据要素交易申请、交易磋商、交易实施、交易结束、争议处理等环节中明确数据信息、内容、用途、交易方式和使用期限等信息，确保符合相关法律、法规、规章和标准等要求。

如发现数据要素交易存在违法违规情形，数据交易服务机构应当依法采取必要的处置措施，并向市数据局等有关主管部

门报告。

各级机构应高度重视数据要素交易模式安全，遵照“原始数据不出域、数据可用不可见”的交易范式，鼓励采用隐私计算等技术手段保障交易安全。

第五十九条 数据要素交易机构应当对拟交易的数据建立分类制度，落实有关部门对不同类别数据提出的安全要求，对拟交易数据建立分级保护机制，根据数据的不同级别，为数据供需双方提供不同强度的安全保护技术支持措施。如交易数据需向境外提供的，应当依法按照国家网信办制定的数据出境安全评估办法进行安全评估。

第十章　风险评估管理

第六十条 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。

第六十一条 市数据安全工作协调机制统一管理、监督和指导数据安全风险评估工作，组织开展相关评估标准制修订及推广应用。各县区主管部门及行业监管部门依据职责分别负责监督管理本地区重要数据和核心数据处理者开展数据安全风险评估工作。

第六十二条 数据责任主体应当建立数据安全防护体系，采

取有效防护措施，提高防篡改、防病毒、防攻击、防瘫痪、防挂马能力，定期进行安全检查和风险评估。对于评估和检查中发现的问题制定整改措施,及时整改,并向归口管理部门报送整改报告。

第六十三条 重要数据和核心数据处理者应每年至少一次风险评估，按照及时、客观、有效的原则开展数据安全风险评估，形成真实、完整、准确的评估报告，并对评估结果负责。

第六十四条 重要数据和核心数据处理者按照国家法律法规、行业监管部门有关规定以及评估标准，对数据处理活动的目的和方式、业务场景、安全保障措施、风险影响等要素，定期开展数据安全风险评估工作。

第六十五条 重要数据和核心数据处理者可以自行或者委托具有相应数据安全工作能力的第三方评估机构开展评估工作。核心数据处理优先使用第三方评估机构开展风险评估。

第六十六条 市政务服务监管局依托政务服务平台确保政务数据“按需归集、应归尽归”，加强政务数据全生命周期质量控制，保障问题数据可反馈、共享过程可追溯、数据质量问题可定责，推动数据源头治理、系统治理，形成统筹管理、有序调度、合理分布的全市一体化政务数据资源体系，形成统一的数据资产，实现信息互通、数据共享。

第十一章 数据安全保障

第六十七条 数据主管部门应加强数据安全保障引导机制，

牵头建立基础保障、技术保障、人员保障以及纪律保障等措施。

（一）基础保障应包含软件保障、硬件保障以及网络链路保障。

1. 软件保障应包含系统加固和数据安全全生命周期管控体系建立，通过消除已知漏洞和增强防护措施，全面提升数据的安全性、完整性和机密性，确保符合法规要求并满足业务连续性要求。

2. 硬件保障应满足物理安全要求，数据中心应具备良好的物理安全措施。关键硬件组件（如电源供应器、硬盘）采用冗余配置，以提高容错率。通过软件与硬件保障之间的协同工作，确保整体系统的安全性。

3. 网络链路保障应确保网络链路传输过程中的机密性、完整性和可用性，通过如 SSL/TLS、IPsec 加密技术保护数据不被窃取，使用如 SM3、SHA—256 的哈希函数验证数据完整性，实施多路径路由和冗余设备提高网络的高可用性和稳定性，采用如双因素认证的强身份验证机制和访问控制策略确保授权访问，建立实时监控和安全威胁响应机制，及时修补已知漏洞，确保网络链路的安全性和可靠性。

（二）技术保障应包含加密与认证技术，采用先进的加密技术保护数据传输和存储过程中的信息安全，并实施身份验证机制，确保只有授权用户可以访问敏感信息。部署日志管理系统和行为分析工具，持续监测系统运行状态，及时发现异常活

动并记录所有访问记录以备审计。

（三）人员保障应明确各部门和个人在数据安全管理中的责任分工，设置数据管理员及数据安全主管等岗位，建立培训教育计划，增强相关人员对数据安全重要性的认识以及技术能力的培养。

（四）纪律审查保障应包含内部审查机制，定期开展内部审核工作:

1. 明确规定工作人员对机密信息和敏感数据的保密责任，包括不得泄露、不得私自复制、不得擅自传输等规定，并设立相应的保密管理制度和流程。

2. 建立严格的数据访问权限控制机制，确保工作人员只能访问其工作职责所需的数据，同时对数据访问进行审计和监控，防止未经授权的访问。

3. 制定工作人员设备使用规范，包括不得私自安装软件、不得访问非法网站不得使用未经授权的设备等规定，确保设备安全和数据保护。

第六十八条 数据责任主体应制定落实数据存储备份和恢复方案，保障相关灾备措施，定期进行灾难恢复演练。数据责任主体应当严格管控移动存储介质的使用，防止移动存储介质在不同网络区域之间交叉使用造成恶意代码的传播和数据泄露。

第六十九条 各县区（工业园区）应保障算力设施平稳运行。

强化算力网络保障，对重要网络设施采用双节点、双路由配置，避免出现单点故障。加强物理设施保护，定期开展巡查巡检，制定应急预案，提高应急处置能力。对重要系统和数据，建立热备双活机制，鼓励应用仿真灰度测试、混沌工程等新技术，发掘并消除软件系统潜在隐患。

第七十条 数据责任主体应严格落实数据安全法律法规要求，开展数据安全防护工作。强化安全技术手段，加强对行为日志、数据流转、共享接口等安全监测分析，推动威胁处置向风险预警和事前预防转变，建立威胁闭环处置和协同联动机制，提升威胁处置科学性、精准性和时效性。

第七十一条 数据主管部门统筹规划数仓建设，坚持“一数一源”，建设“一数一仓”，在各单位管理平台终端建设独立数仓，实现部门数据同仓汇聚、返还、回流、治理、存储、共享。

第七十二条 数据责任主体应坚持总体国家安全观，树立网络安全底线思维，在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储，不得向境外发送。围绕数据全生命周期安全管理，落实数据安全主体责任，促进安全协同共治，运用安全可靠技术和产品，推进政务数据安全体系规范化建设，推动安全与利用协调发展。

第七十三条 政府部门和企事业单位在依法加强安全保障和隐私保护的前提下，建立政府部门和企事业单位等公共数据

资源清单、目录、标准规范及安全保护准则，制定公共数据开放计划，落实数据开放和维护责任，建设全市数据统一开放平台，统筹管理可开放的政府数据资源，提供面向公众的政府数据服务。持续推进政府各部门、企事业单位、社会组织与青海省信用信息系统的数据对接，丰富面向公众的信用信息服务，提高政府服务和监管水平。探索社会化的数据授权运营模式，引导公共数据信息资源的流通合作。

第七十四条 数据主管部门协同各级行业监管部门以及地方管理部门深化统筹联动，建立常态化协调机制加强部门协同，分工做好重点任务组织保障，合力推进数据要素发展及数据安全保障。

第十二章　附　则

第七十五条 对于国家和省级有明确要求的事项，应当严格遵守并执行国家和省级的相关规定。

第七十六条 本办法自2025年5月1日起施行，有效期至2027年4月30日。（自文件发布之日起后30日实施，有效期2年）

附录

名词解释

1. **数据**：是指任何以电子或其他方式对信息的记录。数据在不同视角下表现为原始数据、衍生数据、数据资源、数据产品、数据资产、数据要素等形式。

2. **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的，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。（仅影响组织自身或公民个体的数据一般不作为重要数据。）

3. **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，一旦被非法使用或共享，可能直接影响政治安全的重要数据。（核心数据主要包括关心国家安全重点领域的数据，关系国民经济命脉、重要民生、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。）

4. **一般数据**：是指核心数据、重要数据之外的其他数据。

5. **政务数据**：是指政务部门在履行职责过程中制作或获取的，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的数据等。

6. **社会数据**：社会数据与政务数据相互独立，特指法人主体和自然人在生产生活中生成的数据，如互联网舆情数据、手机信令数据等。

7. **企事业单位信息资源数据：**是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织（以下统称公共管理和服务机构），在履行公共管理和服务职责过程中收集和产生的数据。

8. **无条件开放数据：**是指不涉及敏感信息、个人隐私等重要数据的信息资源，可以在不违反相关法律法规和政策的前提下对外完全开放。这些数据通常是公共信息、基础数据或者已经经过脱敏处理的数据，可以供公众或者其他单位自由获取和使用。

9. **有条件开放数据：**是指一些具有一定敏感性或者隐私性的信息资源，需要在一定条件下才能对外开放。在开放之前，需要对数据进行脱敏处理、权限控制或者签订相关协议等措施，以确保数据的安全性和合规性。这类数据可能包括企业内部的经营数据、客户信息等。

10. **非开放数据：**是指一些涉及重要敏感信息、个人隐私等的信息资源，不应对外开放。这类数据可能包括企业的财务数据、员工的个人身份信息、商业机密等，需要严格保护和控制，避免泄露和滥用。

11. **行业领域数据：**是指在某个行业领域内依法履行工作职责或开展业务活动中产生的数据。

12. **公共数据：**是指各级党政机关、企事业单位依法履职或

提供公共服务过程中产生的数据。

13. **个人信息：**是指以电子或其他方式记录的与已识别或者可识别的自然人有关的各种信息。

14. **衍生数据：**是指经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。

15. **数据交易：**是指数据供方和需方之间进行的，以数据或者数据各类形态为标的的交易行为。

16. **数据流通：**是指数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

17. **数据处理：**包括数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

18. **数据处理者：**是指在数据处理活动中自主决定处理目的和处理方式的个人或者组织。

19. **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理利用的状态，以及具备保障持续安全状态的能力。

20. **隐私计算：**是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私计算的常用技术方案有多方安全计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

21. **可信执行环境：**是指提供基于硬件级的系统隔离和可信

根，支持基于技术信任的数据安全保障能力，保证在安全区域内部加载的代码和数据在保密性和完整性方面得到保护。

22. **联邦学习**：是指多个参与方在不共享原始数据的情况下协作完成机器学习任务的方法。

23. **区块链**：是指使用密码链接将共识确认的区块按顺序追加形成的分布式账本。

24. **关键数据基础设施**：是指支撑国家重要行业和领域中，对于国家安全、国计民生、公共利益具有重大影响的数据系统及其相关设施。这些基础设施包括但不限于数据中心、数据库管理系统、数据传输网络、数据存储设备以及相关的软件和硬件平台。它们在保障数据的完整性、保密性、可用性和可恢复性方面起着至关重要的作用。

25. **信息化项目**：是指以计算机、通信技术及其他现代信息技术为主要手段的公共信息基础设施、信息网络、信息网络安全保障项目；信息资源管理开发应用项目；信息应用系统的新建、扩建、改建和运维；涉及网络互联、信息共享、资源整合、业务协同的信息化项目；数据库和标准体系建设项目；物联网项目等。

表 1　数据级别确定规则表

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据
注：如果影响大规模的个人活组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响。			

表 2 数据安全事件级别与业务损失的严重程度的关系

事件影响对象的重要程度	业务损失的严重程度			
	特别严重	严重	较大	较小
特别重要	一级	二级	三级	三级
重要	二级	三级	三级	四级
一般	三级	三级	三级	四级

表 3 数据安全事件级别与社会危害的严重程度关系

事件影响对象的重要程度	社会危害的严重程度			
	特别严重	严重	较大	较小
特别重要	一级	二级	三级	/
重要	/	二级	三级	四级
一般	/	/	三级	四级

是否宜公开选项：宜公开

抄送：市委各部门，市纪委办公室。

市人大办，市政协办，市监察委，市中级人民法院，市人民检察院。

海东军分区，武警海东支队，海东消防救援支队。

海东工业园区所属园区管委会，各群众团体，青海高等职业技术学院，青海柳湾彩陶博物馆，市属国有企业，省驻市各单位。

海东市人民政府办公室　　2025 年 3 月 31 日印发