

海东市人民政府办公室文件

东政办〔2026〕41号

海东市人民政府办公室 关于印发海东市数据安全应急预案的通知

各县区人民政府，海东工业园区管委会，市政府各部门：

《海东市数据安全应急预案》已经市政府第87次常务会议研究通过，现印发给你们，请认真组织实施。

2026年7月1日

海东市数据安全应急预案

第一章 总则

第一条 目的与依据 为建立健全海东市数据安全事件应急响应机制，提升预防和应对数据安全事件的能力，规范应急处置流程，最大限度减少事件造成的损失和危害，保障数据安全与数字经济健康发展，依据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》《国家网络安全事件应急预案》《海东市数据安全管理办法（暂行）》等法律法规及规定，制定本预案。

第二条 适用范围 本预案适用于发生在海东市行政区域内，或发生在市外但对本市造成影响的各类数据安全事件的预防、监测、预警、响应、处置和恢复等工作。

本预案所称数据安全事件，是指由于人为攻击、技术故障、自然灾害、管理缺失等原因，导致数据遭到篡改、破坏、泄露、丢失、非法获取、非法利用或数据勒索等，从而对国家安全、公共利益，以及个人、组织的合法权益造成危害或潜在危害的事件。

第三条 事件分级 根据数据安全事件的影响对象、危害程度、波及范围和社会影响，将其分为四级：特别重大（Ⅰ级）数据安全事件；重大（Ⅱ级）数据安全事件；较大（Ⅲ级）

数据安全事件；一般（Ⅳ级）数据安全事件。具体分级标准见附件 1。事件分级是启动相应级别应急响应的基本依据。

第四条 工作原则

统一领导，分级负责。在市委、市政府统一领导下，建立健全属地管理、分级负责、分类响应的应急管理机制。事发地人民政府或行业主管部门是处置本地区、本行业数据安全事件的责任主体。

预防为主，平战结合。坚持常态化安全防护与应急处置相结合，强化监测预警、风险评估和日常演练，落实安全防护措施，做好应对准备。

快速反应，协同联动。建立跨部门、跨行业、跨层级的应急联动机制，整合资源，信息共享，形成统一指挥、反应灵敏、协调有序、运转高效的应急处置合力。

科学处置，依法规范。依据法律法规，采用科学有效的技术和管理手段处置事件，及时控制态势、最大限度止损，保护现场证据，第一时间启动应急响应，确保处置工作的合规性。

第二章 安全预防工作

第五条 日常安全管理责任

市数据主管部门统筹协调责任：在市数据安全工作协调机制统一领导下，市数据主管部门牵头统筹全市数据安全工

作，负责拟定总体安全策略和标准规范，监督检查全市数据安全工作落实情况，统筹规划并推动建设市级数据安全监测预警、应急处置等技术支撑平台。同步加强基层数据安全能力建设，提升其对数据分级分类、应急处置等工作的理解和实操能力，夯实基层管理基础。

行业主管部门监管责任：各行业主管部门（如市卫健委、市教育局、市工信局等）负责监督管理本行业、本领域的数据安全工作。落实上级部门制定的行业数据安全指引，督促指导所属单位落实防护要求，并建立本行业应急联络与处置机制。

数据处理者主体责任：所有数据的持有者、管理者、使用者（以下简称“数据处理者”）是数据安全的第一责任人。必须建立健全内部数据安全管理制度，落实数据分类分级保护措施，建成数据分类分级目标信息库，开展常态化安全风险评估与整改，定期组织并参与应急演练和人员培训。配合相关部门（单位）建立数据安全风险清单，协助相关部门（单位）对重要系统和数据资产进行数据安全评估。

第六条 基础安全防护措施 数据处理者应按照数据分类分级保护要求，落实针对性防护措施：对核心数据实施最高级别防护，采用国家密码管理局认可的高强度国密算法加密存储、访问权限严格管控、离线备份等措施；对重要数据强化访问审计、异常行为监控等防护；对一般数据规范管理

流程，确保数据采集、传输、存储、使用、加工、提供、公开、销毁全生命周期可追溯。同时，定期开展安全漏洞扫描和系统升级，及时修补安全隐患，配合上级部门（单位）部署防火墙、入侵检测、数据防泄漏、安全审计等专用防护技术设施。

第七条 应急资源保障 市数据局牵头，会同市发改委、市财政局、市委网信办等部门，规划建设市级数据安全应急资源库，包括专家库、技术工具库、第三方服务商名录等，建立资源调用记录与评估制度，确保应急时可快速调用。各行业主管部门、县区人民政府应结合实际，指导相关行业配套建设本行业、本地区应急资源储备，形成分级保障体系。应急资源库的建设和日常维护更新经费纳入各级财政预算保障。

第三章 应急管理体系

第八条 指挥机构

市数据安全应急指挥部：是全市应对Ⅰ、Ⅱ级数据安全事件的最高临时指挥机构。总指挥由市政府分管数据工作的副市长担任，副总指挥由市数据局局长、市委网信办主任、市公安局分管副局长担任。主要职责：组织领导全市重大数据安全事件应对工作；研究决定应急响应重大决策；批准启动或终止市级应急响应；协调解决处置中的重大问题；必要

时请求上级部门支援。

现场指挥部：根据事件处置需要，由市指挥部或负责Ⅲ、Ⅳ级响应的单位指派成立。负责现场具体处置工作的指挥协调，统筹调配现场应急力量和资源，及时向市指挥部或上级主管部门汇报处置进展。

第九条 办事机构 市数据安全应急指挥部下设办公室，办公室设在市数据局，作为日常办事机构和工作枢纽。主要职责：**1.** 执行指挥部的决策和部署；**2.** 承担应急信息汇总、综合协调工作；**3.** 组织预案编制、修订、演练和宣传培训；**4.** 指导、监督和检查各地区、各部门的应急准备工作；**5.** 组织事后调查评估和总结。

第十条 工作机构与应急技术保障

应急联动单位：包括市委网信办、市公安局、市国家安全局、市委机要和保密局、市工业和信息化局、各行业主管部门、关键信息基础设施运营单位、专业技术支撑机构等。各单位根据职责分工，在指挥部统一领导下参与监测、预警、处置、恢复等各项工作。

市委网信办负责数据安全事件舆情监测、研判与引导、网上舆情管控，统筹网络安全协同处置。市公安局负责涉嫌违法犯罪的数据安全事件（案件）侦查，依法打击数据泄露、篡改、非法获取等违法犯罪行为。市国家安全局负责处置涉及国家安全的数据安全事件。市工业和信息化局负责保障应

急处置期间通信网络畅通，协调运营商切断攻击链路。市委机要和保密局负责统筹数据失泄密事件的保密核查、违规行为查处工作，指导开展失泄密事件应急处置，严守保密纪律，防止泄密范围扩大，依规追究失泄密责任。

应急技术保障：由市数据局牵头组建，负责为应急决策提供技术咨询和专业建议，参与事件研判、处置方案制定、事后评估等工作。同时，联合第三方技术支撑机构，负责应急处置期间的技术研判、漏洞修复、攻击溯源、数据恢复、系统加固等工作，为应急处置提供全程技术保障，解决各类技术难题。

第十一条 分级管理职责

市级层面：市数据安全应急指挥部负责统筹全市数据安全应急管理工作，主导Ⅰ、Ⅱ级事件处置，指导协调Ⅲ、Ⅳ级事件处置。

行业层面：各行业主管部门负责本行业数据安全应急管理，督促落实预防措施，牵头处置本行业领域内发生的Ⅲ级事件，指导本行业Ⅳ级事件处置，及时上报重大风险和事件信息。

县区层面：各县区人民政府负责本行政区域内数据安全应急管理，落实市级部署要求，配合处置跨区域事件，牵头处置本行政区域内发生的、未明确对应行业主管部门的Ⅲ级事件，指导本地区Ⅳ级事件处置。

单位层面：数据处理者负责本单位内部应急管理，落实日常防护和监测责任，先期处置本单位发生的Ⅳ级事件，配合上级部门处置Ⅲ级及以上级别事件。

第四章 预警工作

第十二条 监测体系建设

构建三级监测网络：建立以数据处理者自查为基础、行业主管部门巡查为补充、市级平台监测为核心的三级数据安全监测体系，实现数据安全风险全方位、无死角监测。

落实监测责任：**1. 数据处理者：**负责本单位数据系统与资产的实时监测，利用技术手段对异常访问、数据异常流动、恶意攻击等进行监控，及时发现并处置苗头性风险，定期向行业主管部门报送监测情况。**2. 行业主管部门：**负责对本行业重点单位的数据安全状况进行抽查监测，收集汇总行业风险信息，分析研判行业安全态势，向市数据局报送行业监测报告。**3. 市数据局：**对全市关键数据基础设施、重要数据系统和核心数据加强监管，实现跨部门、跨行业风险关联研判。

第十三条 预警研判 监测发现风险隐患或接获上级、外部预警通报后，相关责任主体应立即组织研判：数据处理者对本单位监测发现的风险进行初步研判，及时处置并上报；行业主管部门对本行业风险信息进行汇总研判，提出行业预警建议；市数据局组织专家对跨行业、区域性重大风险进行

深度研判，确定风险等级（一般、较大、重大、特别重大）和影响范围。

第十四条 预警信息发布

预警责任主体：市数据局是市级数据安全预警信息的发布主体。行业主管部门在发现可能引发跨行业、区域性风险的隐患时，应及时向市数据局提出预警建议。

预警流程：监测发现重大风险隐患或接获上级、外部预警通报后，市数据局组织专家研判，确定风险等级和影响范围，报请市数据安全应急指挥部批准后，通过应急通信系统、官方平台等渠道发布预警信息。预警信息应包括风险性质、可能影响、建议措施和预警期限。

预警调整与解除：根据风险变化情况，发布主体可适时调整预警等级或延长预警期限；当风险得到有效控制、隐患消除后，经研判确认，及时发布预警解除信息。

第十五条 预警响应措施 预警信息发布后，各相关单位应立即采取响应措施：数据处理者强化监测防控，开展风险排查整改，做好应急准备；行业主管部门加强行业巡查指导，督促相关单位落实防护措施；市数据局统筹协调技术支撑力量，做好应急资源调配准备，必要时组织开展专项防控工作。

第五章 应急响应

第十六条 响应启动主体与条件

响应启动主体：遵循“分级负责、属地为主”原则。Ⅰ、Ⅱ级响应：由市数据安全应急指挥部决定启动。Ⅲ级响应：由事件主要影响的行业主管部门或事发地区（县）人民政府决定启动，并报市数据局备案。Ⅳ级响应：由事发单位或其上级主管部门决定启动，并按照行业管理要求上报。

响应启动条件：事件发生后，经初步研判符合附件1中相应级别的标准，或发生数据失泄密、密码泄露、违规使用密码等情形，即应启动对应级别的应急响应。启动响应时，需明确响应级别、启动时间、响应范围、牵头单位及参与单位等核心信息。

第十七条 响应等级调整与终止

响应调整：应急处置过程中，经研判发现事件影响范围扩大、危害程度加剧，超出当前响应级别应对能力的，应及时提升响应级别；若事件得到有效控制，影响逐步缩小，可降低响应级别。级别调整由原启动主体决定并发布。

响应终止：当事件处置完成、风险消除，核心业务恢复正常，经牵头处置单位组织研判确认后，由原启动主体决定终止应急响应，并发布终止信息。

第十八条 响应期间统筹协调 响应启动后，牵头处置单位应立即组建工作专班，统筹推进应急处置工作：明确各参与单位职责分工，建立每日会商机制，及时汇总处置进展；

协调调配应急资源，保障技术、人员、物资等需求；及时向上级部门汇报事件处置情况，必要时请求支援。各参与单位应服从统一指挥，密切配合，形成处置合力。

第六章 应急处置

第十九条 先期处置与报告

事发单位：立即采取隔离受影响系统、暂停相关服务、保护现场日志和数据备份、封堵安全漏洞、冻结异常密码账号、切断泄密渠道、严控涉密数据流转等措施控制事态扩大，并在 30 分钟内向行业主管部门和市数据局电话初步报告，1 个工作日内提交书面报告（特殊紧急情况可先行口头报告，后续补报书面材料）。报告内容详见附件 3。

行业主管部门/事发地区政府：接报后迅速核实情况，指导事发单位先期处置，及时汇总事件信息，按规定向上级报告；涉及跨部门、跨区域的，及时通报相关单位协同处置。

市数据局：接报 I、II 级事件或重大 III 级事件后，立即向市数据安全应急指挥部汇报，同步组织技术力量介入研判，做好应急处置准备。

第二十条 现场处置核心措施 成立现场应急指挥部，统一协调指挥现场处置力量。指挥部由牵头响应单位负责组建或市数据安全应急指挥部指定，相关单位派员参加，明确现场指挥、技术保障、安全保卫、舆情应对、失泄密管控、

密码处置等专项工作组职责。

技术处置：技术保障团队立即介入，开展攻击溯源、漏洞分析、病毒查杀等工作，定位事件根源；采取数据恢复处置、系统安全加固、访问策略优化、账号密码紧急重置、违规权限即时回收、涉密数据隔离管控等技术措施，消除安全隐患，防止事件二次发生，同时开展数据安全应急溯源与深度复盘分析。

案件查办：公安机关对涉嫌犯罪的行为依法开展侦察，固定犯罪证据，对犯罪嫌疑人依法采取强制措施。

舆情应对：市委网信办同步启动网络舆情监测与管控，防范网上负面舆情扩散蔓延。

第二十一条 损失控制与业务恢复

损失评估：处置单位及时评估事件影响范围、数据损毁或泄露情况、业务中断损失及对个人、组织合法权益的危害，形成损失评估报告，为后续处置和赔偿补救提供依据。

业务恢复：处置单位优先恢复民生保障、公共服务、政务服务等关键业务，启用备份数据和备用系统，确保核心服务不间断；非关键业务逐步有序恢复，恢复过程中强化安全监测，防止风险反弹。

补救措施：处置单位对受影响的个人和组织，依法依规履行通知义务，告知风险防范措施；对造成损失的，协助相关单位做好赔偿、补偿等善后工作；涉及个人信息泄露的，

按规定向有关部门报告并通知受害人。

第二十二条 重大事件统筹处置 对于涉及多个部门、影响广泛的复杂事件，市数据安全应急指挥部统筹调度全市资源，采取包括但不限于以下措施：指令相关区域或行业采取临时性管控措施；协调提供跨域应急技术支援；调配市级应急资源库中的专家、技术工具和备用资源；根据需要请示省级部门或兄弟市州提供支持。

第七章 后期处置

第二十三条 事件评估 应急处置结束后 5 个工作日内，牵头处置单位组织相关部门、专家和事发单位，对事件原因、应急处置过程、损失影响、暴露问题等进行全面评估，形成评估报告。评估报告应包括事件基本情况、处置措施及成效、存在的问题、改进建议等内容，按程序上报市数据主管部门并归档。

第二十四条 总结改进 事发单位应在事件处置完成后一周内，结合评估报告形成总结报告，梳理应急处置中的经验与教训，提出针对性改进措施。

各相关单位根据评估报告和总结情况，明确责任认定，提出整改要求和责任追究建议；对违反法律法规和本预案规定，未履行应急管理责任，导致事件发生或处置不力的单位和个人，依规依纪依法追究 responsibility。

建立年度总结报告制度：各行业主管部门、县区人民政府每年向市数据局报告本行业、本地区数据安全事件处置情况及应急管理工作的开展情况，市数据局汇总后向市政府汇报。

第八章 附则

第二十五条 预案管理与更新 本预案定期组织评估和修订。各县区、各行业主管部门应参照本预案制定本地区、本行业的实施细则，并报市数据局备案。

第二十六条 实施时间 本预案由市数据安全工作协调机制办公室负责解释，自发布之日起施行。

附件 1

海东市数据安全事件分级标准

级别	判定标准（满足任一条件）
特别重大 （ I 级）	1.核心数据大规模泄露、篡改或丢失，数据量≥100 万条，或涉及≥60 万人敏感个人信息；2.核心数据存储/处理设施（ 市级算力核心节点、可信数据空间 ）瘫痪≥24 小时，导致全市核心政务服务、重点民生保障业务完全中断；3.直接经济损失≥1 亿元；4.可能危害国家安全，或引发跨区域群体性事件；5.国家、省级通报的特别重大数据安全事件。
重大（ II 级）	1.核心数据局部泄露、篡改或丢失，数据量 50 万-100 万条，或涉及 10 万-60 万人敏感个人信息；2.重要数据大规模泄露、篡改或丢失，数据量≥500 万条，或涉及 ≥500 万人个人信息；3.重要数据存储/处理设施瘫痪≥12 小时，导致区域性核心业务、重点民生服务中断；4.直接经济损失≥2000 万元；5.可能引发区域性恐慌或社会秩序混乱；6.省级通报的重大数据安全事件。
较大（ III 级）	1.重要数据局部泄露、篡改或丢失，数据量 100 万-500 万条，或涉及 1 万-10 万人敏感个人信息；2.一般数据大规模泄露、篡改或丢失，数据量≥1000 万条，或涉及 ≥100 万人个人信息；3.数据存储/处理设施故障≥6 小时，影响单个行业或单个县（ 区） 核心业务、民生服务；4.直接经济损失≥500 万元；5.造成较大社会影响，引发局部舆情关注。
一般（ IV 级）	1.一般数据少量泄露、篡改或丢失，数据量 < 100 万条，或涉及 < 1 万人个人信息；2.数据存储/处理设施故障 2-6 小时，影响范围有限；3.直接经济损失 < 500 万元；4.影响较小，未引发舆情或仅引发局部轻微关注。

附件 2

应急处置流程操作表

流程 序号	处置阶段	具体操作内容	责任主体	完成时限	关键输出物	异常情况处 理措施
1	风 险 监 测 与 核 实	1.通过日志审计、流量分析、安全监测平台监控捕捉异常数据行为；2.现场核验异常真实性，排除误报；3.初步判断事件类型（泄露/篡改/故障）及影响数据级别（核心/重要/一般）。	数据处理者	10 分钟内	《数据安全事件初核记录表》	若无法即时核实，立即启动备用监测终端，15 分钟内必须反馈初核结果。
2	先期处置、 级 别 初 判 与 上 报	1.立即采取隔离系统、暂停服务、保护日志与备份、封堵漏洞、冻结账号、切断泄密渠道、管控涉密数据等先期处置；2.对照分级标准初判事件等级；3.按规定向行业主管部门和市数据局报告。	事发单位	30 分钟内	《数据安全事件级别初判意见书》《事件上报单》	若初判等级存疑，先按高一级别上报，避免延误；若上报渠道中断，越级报告。
3	应 急 响 应 启 动 与 处 置 方 案 制 定	1.按分级管理权限启动对应级别应急响应；2.成立现场指挥部，明确分工；3.技术保障团队制定专项处置方案。	事发单位或其 上级主管部门 （Ⅳ级）/事件 主要影响的行 业主管部门或 事发地区（县） 人民政府（Ⅲ 级）/市数据安 全应急指挥部 （Ⅰ/Ⅱ级）	1 小时内	《应急响应启动通知书》《专项处置方案》	技术瓶颈立即启用专家团队，2 小时内确定替代方案。
4	技 术 处 置 与 事 态 控 制	1.开展攻击溯源、漏洞分析、病毒查杀，定位事件根源；2.采取数据恢复、系统加固、访问策略优化、账号密码紧急重置、违规权限回收、涉密数据隔离管控；3.消除隐患、防止事件反弹复发；4.同步开展溯源与深度复盘分析。	技术保障团队	Ⅰ/Ⅱ级：4 小时内 Ⅲ/Ⅳ级：2 小时内	《技术处置过程记录表》《攻击溯源报告》	若备份数据损坏，立即协调灾备数据，同步联系第三方机构开展数据恢复。

5	事态验证与损失评估	1.数据完整性校验、系统运行测试、风险核查；2.开展事件影响范围、数据损毁、业务中断、经济损失等评估。	应急响应实施团队	处置完成后1小时内	《数据完整性校验报告》《系统恢复验证单》《损失评估报告》	若验证发现数据不完整，立即补充采集，2小时内完成补全。
6	应急响应终止	事件处置完成、风险消除、核心业务恢复正常，由原启动主体研判确认后终止响应，并发布终止信息。	原响应启动主体	验证通过后30分钟内	《应急响应终止通知书》	若申请被驳回，返回“技术处置”阶段，针对性补充措施，12小时内重新提交申请。
7	事后评估、总结与归档	1.牵头处置单位5个工作日内完成事件评估；2.事发单位一周内提交总结报告；3.完善档案、落实整改；4.归档留存。	牵头处置单位、事发单位	终止后24小时内归档 评估：5个工作日 总结：一周内	《数据安全事件处置档案》 《改进措施清单》	若档案缺失关键材料，立即联系责任团队补充，48小时内必须完成归档，否则纳入年度考核负面清单。

附件 3

数据安全事件标准化报告模板

一、事件基本信息

1. 事件发生时间：____年____月____日____时____分
2. 事件发生地点（系统/平台名称）：_____
3. 事件类型（泄露/篡改/丢失/破坏/非法获取）：____
4. 影响数据级别（核心/重要/一般）：_____
5. 事发单位及联系人：_____联系电话：_____
6. 属地管理部门：_____联系人：_____联系电话：_____

二、事件初步情况

1. 影响范围（涉及数据量、人员/企业数量、区域）：_____

2. 初步危害评估（国家安全/公共利益/经济损失/个人权益）：_____

3. 已采取的先期处置措施：_____

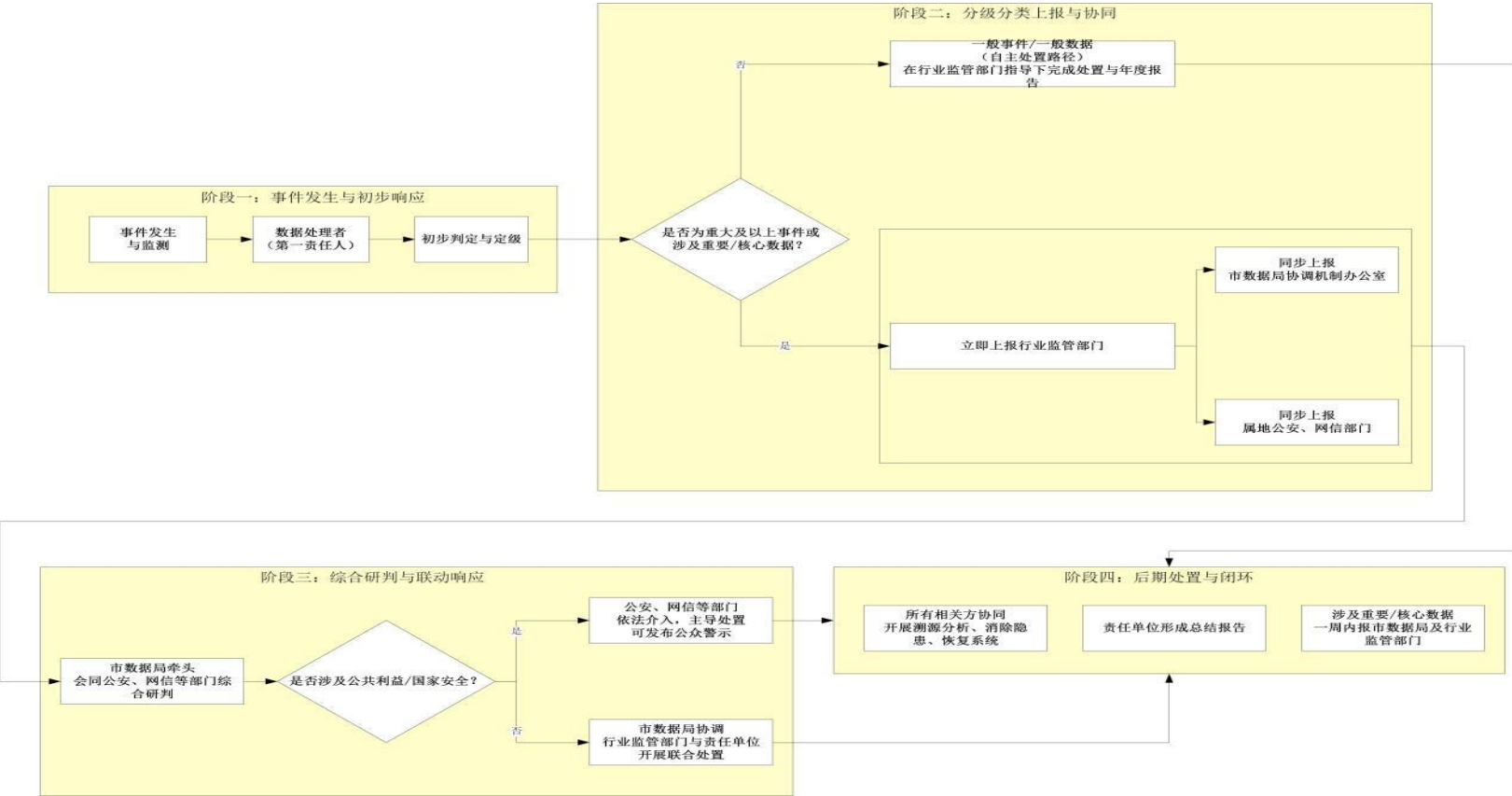
三、后续需求及建议

1. 所需应急资源（技术/人员/物资）：_____

2. 建议响应级别及处置方向：_____

报告人：_____ 报告时间：____年____月____日____时

数据安全事件应急处理流程图



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

2026 年 7 月 1 日印发
