附件

2026年交通运输、气象服务领域数据流通安全治理典型案例

2026年5月

目 录

数据流通安全治理典型案例（交通运输领域）.....1
基于交通安全预警云哨系统的ETC门架数据流通安全应用案例.....2
基于交通行业船舶数据流通利用场景的数据沙箱技术应用案例.....5
基于港口集装箱进提箱业务场景的跨主体数据流通安全应用案例.....8
基于港航供应链船舶靠泊调度跨主体数据协同场景的数据流通安全应用案例.....11
基于北港网平台港口数据流通场景的安全规则体系应用案例.....14
数据流通安全治理典型案例（气象服务领域）.....17
基于金融气象数智化服务场景的气象数据流通安全应用案例.....18
基于跨行业一网统管场景的交通和气象数据流通安全应用案例.....21
基于气象数据跨平台交易场景的数据流通安全技术应用案例.....24
基于风电场站吊装作业场景的气象数据流通安全应用案例.....27
基于气象数据滥用防范场景的数字信封安全技术应用案例.....30
基于三峡防洪和水电调度场景的气象数据流通安全应用案例.....33

数据流通安全治理典型案例

（交通运输领域）

基于交通安全预警云哨系统的ETC门架数据流通安全应用案例

一、数据流通场景和安全治理挑战

在ETC门架数据流通场景中，面临数据跨主体流通合规难、数据全流程防护难、跨主体协同监管难等问题。湖南省高速公路联网收费中心（以下简称“湖南联网中心”）与湖南省公安厅交通管理总队（以下简称“湖南公安交管”）深化ETC门架数据协同，确定数据“最小化原则”，仅传输车辆号牌、通行时间、行驶速度等必要信息，联合构建交通安全预警云哨系统，实现高速公路疲劳驾驶、超速行驶等违法行为监管。

该案例场景中的业务流程为，湖南联网中心作为数据提供方，通过ETC门架、收费站及卫星定位平台采集车辆通行流水、门架经纬度、两客一危一货卫星定位数据等多源数据，在源头完成疲劳驾驶和超速行为预分析，将疑似数据按照“最小化原则”推送至DMZ安全缓冲区，再通过光纤专网加密共享至湖南交管云哨系统；湖南公安交管对疑似数据进行实时复核计算，依据执法规则触发预警提示，并将处置结果反馈系统用于模型优化。

上述场景中存在安全治理挑战，一是数据跨主体流通的安全合规依据缺乏，跨主体管理权责边界模糊；二是全链路数据安全技术防护存在局部短板，数据存在泄露风险；三是跨主体数据流通机制

尚未标准化，数据流通中存在数据被篡改等风险。

二、安全治理措施

（一）明权责定标准，夯实合规治理基础。针对跨主体流通安全合规和权责边界，依据交通运输部、公安部《关于开展公路运行监测数据共享共用工作的通知》（交办规划〔2024〕72号）相关要求，双方签订《数据共享与安全保密协议》，明确湖南联网中心负责数据采集源头的质量管控、最小化筛选并推送至DMZ缓冲区；湖南公安交管负责云哨系统数据存储、分析及安全防护；双方设定数据留存期限，到期自动销毁。

（二）技术赋能实现全链路安全防护。依托完成网络安全等级保护要求（三级）备案及测评的云哨系统，在采集环节建立数据血缘图谱，校准门架经纬度，将漏采率控制在5%以内；在传输环节依托光纤专网实施端到端加密；在存储环节对车辆号牌、卫星定位等数据按照符合国家标准的商用密码算法加密存储；在应用环节引入权限模型，湖南公安交管下属各支队仅能访问其管辖范围内的数据；在审计环节部署日志审计系统，完整记录数据访问、预警触发等行为。

（三）完善跨域协同机制，保障流通数据的高效处置。双方联合建立协同应急处置机制，严控数据使用权限与时效，杜绝违规复用、二次流转。压实双向安全权责，健全全流程溯源审计、应急处置与留存归档机制，明确数据安全事件上报流程与责任分工，全程保留数据使用与销毁记录，接受常态化监督，形成数据流通全生命

周期安全管控闭环。

三、典型意义和安全治理成效

通过“权责明确+技术赋能+标准化跨域流通”的治理模式，有效解决了数据流通中的合规、安全、跨域协同难题，实现数据合规使用、安全防护提升、执法效能提高。可有效杜绝非法访问，提升疲劳驾驶违法行为发现率，提高超速违法行为处置效率。该案例示范价值突出，打破了交通管理与高速运营的行业数据壁垒，构建了可复制、可推广的数据安全治理模式，为全国高速公路 ETC 数据安全流通及交通安全智能化监管提供了实践样本。

基于交通行业船舶数据流通利用场景的数据沙箱技术应用案例

一、数据流通场景和安全治理挑战

船舶行业是交通运输领域数据要素密集型行业，船舶能效与碳核算数据流通场景面临数据分散、泄露风险高、安全与价值难以平衡等问题，制约行业绿色低碳转型。北京海泰方圆科技股份有限公司以自主可控的商用密码、数据沙箱、联盟链为底座，为中国船级社数字空间提供技术支撑，构建“可用不可见”的安全流通环境，为数据跨主体流通利用提供安全保障。

该案例场景中的业务流程为，船东、船舶管理公司、港口运营方等数据提供方实时采集航行、燃油消耗、设备运行等数据并统一归集至中国船级社运营的数据服务平台；数据服务平台将原始数据导入数据沙箱，由数据加工方（能效算法服务商）在沙箱内完成碳核算、能效对标、合规评估等计算；计算完成后仅输出脱敏结果，供航运企业、海事监管部门、节能服务机构等数据需求方用于决策支撑、监管核查与合规申报。

上述场景中存在安全治理挑战，一是敏感的船舶能效与碳排放数据跨主体流通泄露风险高，导致企业不愿共享，制约产业链协同；二是传统脱敏技术降低数据精度，无法支撑碳核算与能效评估，安全合规与数据价值难以兼顾；三是在船舶能效与碳核算数据的加工

处理过程中，存在越权访问、操作溯源缺失、安全事件处置不及时等风险。

二、安全治理措施

（一）以全链路加密与安全隔离，确保数据“可用不可见”。建立全链路加密与隔离通道，采用自主可控的商用密码算法对船舶能效与碳排放数据全链路加密并保留数据原格式。依托数据沙箱构建隔离域，集成虚拟可信平台模块，保障原始数据在可信边界内进行计算，实现数据“可用不可见”。

（二）以数据脱敏和高保真合成数据，兼顾安全与价值释放需求。依托船舶行业数据特征库与深度学习模型，在数据沙箱内，对接入船舶碳计算所需的航行轨迹、能耗记录等关键数据源，实施动态脱敏处理，完整保留能效与碳核算统计特征。在沙箱内生成高保真合成数据，无需调用原始数据即可支撑碳核算建模，兼顾合规安全与计算精度需求。

（三）以行为管控、安全审计和应急响应机制，保障数据全流程安全可控、可审计。依托策略引擎对船舶能效与碳核算数据执行字段级权限管理，权限申请实行双人复核、上链存证、限时自动失效管理。同步开展全流程安全审计，将数据接入、调用、核算、审核、导出等全流程操作日志实时写入联盟链，通过签名存证和长期保存，确保操作记录不可篡改，支持第三方在线核验。依托数据沙箱对数据实行入箱管控，内置异常监测与权限熔断机制，一旦监测到异常行为即刻自动阻断并开展快速核查处置。

三、典型意义和安全治理成效

通过构建“数据可用不可见、碳值可核算、过程可审计”的船舶能效与航运碳核算数据安全流通治理模式，有效破解航运绿色合规数据共享信任壁垒，为海事绿色低碳监管、国际航运合规提供可复制实践样本。项目成功接入碳计算 8 大关键数据源，覆盖 5200 余艘营运船舶能效数据，实现跨系统、跨地域可信数据共享。安全治理成效显著，数据泄露风险概率显著降低；合规审查效率大幅提升，审查周期缩短至 2 天；试点参与企业由 3 家增至 12 家，数据共享意愿明显提升；企业数据流通安全信心显著增强，对交通行业绿色低碳数据流通场景具备重要示范价值。

基于港口集装箱进提箱业务场景的跨主体数据流通安全应用案例

一、数据流通场景和安全治理挑战

在港口集装箱业务数据流通场景下，面临多方主体职责不清、传输安全能力薄弱、权限管控不足等难题。在广西北部湾国际港务集团有限公司（以下简称“集团”）的统筹规划下，广西钦州保税港区宏港码头有限公司（以下简称“宏港码头”）发挥自动化码头技术优势，协同码头客户，通过开展港口集装箱数据流通安全治理，保障数据安全流通，释放数据价值。

该案例场景中的主要业务流程为，货代、船代等码头客户作为数据提供方，在集团“在线业务服务平台”录入业务信息；集团“电子数据交互平台”作为数据汇聚与转发方，对数据进行标准化处理后，依据作业码头信息推送至宏港码头“生产管控平台”；“生产管控平台”作为数据加工方，联动设备控制系统、智能闸口系统等，调度自动化设备完成装卸与堆存作业；业务办结后，码头客户作为数据需求方，从码头获取脱敏后的作业结果，支撑下一物流节点使用，形成数据“采集—传输—加工—应用”的闭环。

上述场景中存在安全治理挑战，一是多方主体在数据流通各环节的管理职责缺乏清晰界定，责任追溯难；二是数据跨系统、跨网络传输存在薄弱点，存在数据被窃听、篡改或伪造的风险；三是系

统应用层权限管理不足，难以实现最小必要的权限管理，数据操作缺乏有效约束。

二、安全治理措施

（一）**协议明责，闭环管控**。客户、集团、码头逐层签订数据安全协议，明确各方主体在数据全生命周期管理的安全职责，客户履行数据提供与合规使用义务，集团负责保障数据传输过程安全，宏港码头承担数据在码头园区内的加工合规与流转安全的管理职责。各方遵循“最小必要原则”，将安全要求内嵌于制度、业务流程及系统设计，制定企业级《数据分类分级管理办法》，确保数据采集、传输、使用等环节权责清晰、合规可控。

（二）**统一通道，多层防护**。数据统一经由集团电子数据交互平台进行交换，采用标准接口对接，杜绝非正式传输渠道；部署专用传输链路，确保集团与码头数据交换不出内网；采用加密算法对传输数据进行加密，防止窃听与篡改；部署 API 网关，实现接口身份认证、流量控制与行为审计。

（三）**物理隔离，全程管控**。针对码头系统运行环境，进行网络区域的安全划分和隔离，划分“生产网、办公网、视频网”，通过防火墙进行三网安全隔离，在生产网内设置访问控制策略，仅允许经审批的访问申请，并按照白名单策略控制数据交换。部署支持自主可控的商用密码算法的 VPN 及堡垒机，部署态势感知、数据库加密机、工控安全卫士等防护设备，搭建纵深防御体系，实现多方位安全防护；依据分类分级标签对即时通讯、邮件等外发渠道实

时监测与阻断，将数据加工能力内置于码头平台，客户通过安全接口在线查询、下载经脱敏的业务数据，支撑后续物流流转，形成数据应用安全闭环。

三、典型意义和安全治理成效

通过构建“协议明责、统一通道、安全隔离、全程管控”治理框架，系统性解决了港口数据流通责任难界定、传输难防护、扩散难管控的共性痛点，形成了可复制的安全治理路径。基于安全可信的数据流通环境，进提箱业务办理效率大幅提升，进提箱作业时长显著缩短。本案例以数据安全治理赋能西部陆海新通道贸易畅通，为多主体协同场景提供了安全与效率并重的实践参考。

基于港航供应链船舶靠泊调度跨主体数据协同场景的数据流通安全应用案例

一、数据流通场景和安全治理挑战

在港航数据流通应用场景下，普遍存在跨主体数据标准不统一、数据开放共享与安全防护失衡等痛点，制约船舶靠泊调度效率与供应链整体安全。日照港集装箱发展有限公司（以下简称“日照港”）作为区域核心港口运营与数据枢纽主体，联合船公司、引航站等多方主体，构建港航跨主体数据安全协同流通体系，支撑船舶智能靠泊调度与高效作业。

该案例场景中的业务流程为，船公司、引航站将船舶动态、作业计划等供应链数据脱敏后推送至日照港建设的港口数据安全平台；日照港完成数据融合分析与智能调度计算，形成最优靠泊方案与作业指令再将结果进行回传，实现脱敏入域、安全分析、合规出域的全流程协同作业。

上述场景中存在安全治理挑战，一是港航跨主体数据安全标准不统一，船舶、港口、引航数据分类分级规范缺失，缺乏统一合规管控依据；二是港航高频实时数据传输链路开放，船舶动态、作业指令等数据存在传输数据泄露、篡改、非法劫持等风险；三是港口关键数据访问量大，授权访问、运维操作管控粗放，数据泄露风险高，缺乏常态化安全运营和保障机制。

二、安全治理措施

（一）建立港航场景化数据安全管理制度体系。依据《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等法律法规，联合船公司、引航站制定港航靠泊调度数据分类分级规范、数据全生命周期管理办法等标准，明确数据权责、流转规则、安全要求与责任边界，形成统一、可落地的跨主体安全管理标准。

（二）构建全链路数据安全技术防护体系。建立数据分类分级差异化防护机制，对港航业务数据定级为一般数据，再细分为1级、2级、3级实施差异化管控，1级数据强化边界隔离与身份鉴别，2级数据落实接口鉴权、加密传输、全程追溯，3级数据采用专线或加密信道传输、数据脱敏、细粒度权限控制，并开展传输前风险评估备案；适配港航高频实时交互特点，实行数据按需脱敏，全链路加密，依托定制化API审计实现传输监控溯源，同步优化作业高峰风险识别模型，严格执行最小权限管理。

（三）建立常态化数据安全风险监测与应急保障机制。建立港航数据安全日常巡检、风险监测、事件响应、复盘改进的常态化运营机制，定期开展漏洞扫描、渗透测试与应急演练；明确授权访问、运维操作的规范与审批流程，实现数据权限最小化、数据操作可审计、数据风险可监测。

三、典型意义和安全治理成效

通过构建港航跨主体数据协同安全流通模式，规范船公司、引航站、港口等跨主体数据共享交互边界，在保障安全前提下打通数

据壁垒，实现安全可控的数据流通共享，稳定支撑船舶靠离泊协同调度，保障数据库、数据表安全运行。安全治理措施实施以来，有效防范生产中断、数据外泄等风险，显著提升跨主体协同效率。在安全护航下，大幅压缩船舶在港待泊及锚地等候时间，码头泊位利用率有所提升，为全国港航领域数据流通安全治理提供可复制、可推广的实践范式。

基于北港网平台港口数据流通场景的安全规则体系应用案例

一、数据流通场景和安全治理挑战

在港口数据流通场景中，需打破物流全链条数据壁垒，提升跨领域数据高效融合与安全水平。依托西部陆海新通道建设的战略机遇，北港网统一客户服务平台（以下简称“平台”），致力于打通物流全链条的数据壁垒，推动数据的高效融合与安全共享，从而持续提升北部湾港的综合服务能力和现代化运营水平。

该案例场景中的主要业务流程为，船公司、码头等单位作为数据提供方，通过 EDI（电子数据交换）或 API 将业务指令与状态数据推送至平台；依托平台对多源数据进行整合、清洗与标准化处理，生成作业指令并分发给数据使用方；运输公司通过北港通 APP 获取作业指令、完成进出闸预约；海关作为监管方，接收预约报文核验并触发抬杆放行。作业数据再回传平台形成了“采集—加工—分发—执行—反馈”的数据闭环。

上述场景中存在安全治理挑战，一是跨主体数据标准不统一，数据交互低效、责任界定难，数据共享存在合规风险；二是数据来源可靠性不足，传统依赖纸质指令的业务模式，存在数据易被篡改、伪造且难以全程追溯的问题；三是多方系统安全能力参差不齐，人员管控粗放，安全监测不完善，存在安全事件溯源难的问题。

二、安全治理措施

（一）规范统一数据共享管理规范，统筹数据交互标准与格式协议。制定北部湾港统一 EDI 报文规范，明确字段、格式与协议；建立覆盖数据全生命周期的数据管理体系，对数据进行采集、传输、存储、使用、共享、销毁等环节的标准化管控。建立覆盖数据全生命周期的常态化管控机制，明晰各参与主体权责边界，规范数据共享流转全流程。

（二）构建数据安全防护与全链路追溯能力，全方位安全纵深防护管控。将电子放货数据上链存证，记录全流程操作日志，确保不可篡改、全程可溯；建立涵盖身份认证、权限核验与数据格式校验的三重访问控制机制，建立纵深防御与协同响应体系，实现全天候威胁监测与实时告警处置。

（三）建立人员权限精细管控与多方应急协同机制。落实分级权限管理机制，在内部管控方面，严格执行权限审查、最小权限分配及离职权限及时回收；在外部协同方面，深化跨主体安全协同，推动各方安全协议标准化，实现主体间的数据安全交换与策略联动。建立联合应急预案，定期组织多主体参与应急演练，模拟数据恢复、接口攻击等典型场景，确保事件发生时能快速隔离风险、高效协同恢复。

三、典型意义和安全治理成效

通过构建“标准先行—技术保障—生态共治”全流程数据安全治理体系，确保数据上链存证不可篡改、全程可溯，打通了港口、

船公司、码头等物流数据壁垒，促进港口数据的高效融合与安全共享。自安全治理措施实施以来，集装箱受理办理时效压缩至1分钟内，集卡闸口通行控制在30秒内，运行效率大幅提升，实现数据安全事件零发生，全面筑牢港口数据安全坚固防线。

数据流通安全治理典型案例

（气象服务领域）

基于金融气象数智化服务场景的气象数据流通安全应用案例

一、数据流通场景和安全治理挑战

当前金融气象服务领域面临气象数据与金融业务融合不足、合规流通机制缺失等挑战。上海金融气象创新中心推动上海华云实业有限公司和上海数字产业（集团）有限公司联合成立“上海金融气象领域气象数据要素联合运营中心”（以下简称“联合运营中心”），建设“金融气象数智化服务平台”，旨在将金融气象指数产品及预报、预警、评估等气象数据要素，安全、合规、高效地流通至银行、保险、证券等金融机构，开发并提供高价值数据产品与服务。

该案例场景中的业务流程为，气象部门提供可授权运营的公共气象数据，通过“金融气象数智化服务平台”进行脱敏等合规处理后，经联合运营中心授权运营，由以上海市联合征信有限公司为代表的科技企业入驻平台，开发形成金融气象指数等数据产品，再通过平台向金融机构交付，实现跨主体、可控可追溯的数据流通路径。

上述场景中存在安全治理挑战，一是金融气象场景多元创新，气象数据流通缺乏针对性制度与评估标准，供需双方流通存在合规顾虑；二是多主体参与气象数据运营加工，权责边界模糊，缺少动态约束机制；三是跨主体流通链条长，数据泄露、滥用及追溯难等安全风险突出。

二、安全治理措施

（一）法治引领，奠定数据合规流通制度体系。依托浦东新区法规立法授权优势，出台全国首部气象数据要素领域的地方性管理文件《浦东新区促进气象数据要素市场化发展若干规定》，为气象数据合规流通提供制度依据：以“开放程度更高的共享目录”扩容数据资源供给，以“分级授权运营模式”鼓励市场多元主体参与；配套制定《浦东新区气象数据授权运营应用场景合规性评估细则》，强化合规前置审核，对数据应用场景开展准入评估，从源头降低气象数据流通风险。

（二）机制管理，明确数据流通安全责任体系。制定《上海金融气象领域气象数据授权运营实施方案》，明确气象数据“实施机构—运营机构—开发机构”的权责边界：上海金融气象创新中心作为实施机构提供技术支持和内部审计，防止气象数据资源不当进入市场；联合运营中心作为运营机构开展数据安全管理，避免超授权使用和数据安全风险；开发机构确保数据加工全过程符合安全和合规标准。配套建立多维度年度评估动态管理机制，将评估结果作为再次申请授权的依据。

（三）技术赋能，筑牢数据流通安全防线。通过分布式部署、数字身份标识与多维度安全供给架构，搭建数据流通安全技术平台。一是采用“内网+互联网”双节点部署架构，数据按照敏感度分级存储于不同节点服务器，通过加密技术进行数据同步，确保跨区域数据传输不被非法截取。二是数据产品流通前上传气象部门“气象

数据流通安全监管平台”获取气象数据身份标识，确保每一步操作均可追溯，防止数据被非法留存或滥用。三是面向多元化数据供给需求，构建多维度安全供给架构，分别使用 API 接口、脱敏处理、可信数据空间等形式，实现各应用场景下数据全流程安全、高效、合规供给与应用支撑。

三、典型意义和安全治理成效

通过“合规化处理+场景化供给”模式，构建“技术控险+制度定责+监督闭环”治理框架，实现气象数据多渠道高效利用的全链路安全闭环，为金融气象数据要素安全流通提供实践参考。安全治理措施已应用于多家保险、银行等金融机构，支撑车险风控、气候投融资评估等多场景安全落地，显著提高气象数据供给效率，助力金融机构赋能农业、能源、电力等实体经济高质量发展，为气象数据要素跨领域安全流通、多渠道合规利用，提供可复制、可推广的实践范式。

基于跨行业一网统管场景的交通和气象数据流通安全应用案例

一、数据流通场景和安全治理挑战

在高速公路交通气象服务场景中，存在多种监测数据跨行业跨地域流通难、数据安全保障难、恶劣天气应急处置效率低等难题。安徽省公共气象服务中心（以下简称“公服中心”）和安徽气象信息有限公司（以下简称“气信公司”）共同建立气象观测站数据、道路信息与视频监控数据统一管理机制，打造天气监测、数据传输、气象预警、应急处置业务安全闭环。

该案例场景中的业务流程为，安徽省公安厅交通管理总队（以下简称“交管总队”）及各市交管支队按每 10 分钟频次提供交通视频图像，安徽省交通运输综合执法监督局（以下简称“交通执法局”）提供路网、道路管控、车流量数据，公服中心按每 1 分钟频次采集气象、道面状态等观测数据。多源数据经合规处理、安全汇聚、融合加工后，通过气信公司建设的安徽省高速公路恶劣气象条件监测预警系统进行安全共享。公安交管、交通运输等部门用户通过加密授权技术获取认证后使用数据和产品。

上述场景中存在安全治理挑战，一是数据涉及气象、交通、公安部门，协同治理难，权责边界模糊，易引发数据泄露；二是视频、路网、气象等多模态数据结构复杂，脱敏难度大；三是跨主体数据

共享存在合规隐患，数据传输环节多，服务产品数据传输存在数据泄露风险。

二、安全治理措施

（一）遵循数据治理制度体系，明晰安全规则。落实安徽省气象局《气象数据共享服务与安全管理办法》《气象数据安全审查细则》等要求，按照数据分类分级和用户分类规范开展交通气象数据共享，依托气象数据流通安全监管平台实现交通气象数据全生命周期监管，有效保障数据安全。联合安徽省公安厅、交通运输厅制定《关于全省高速公路全程视频监控管理系统优化完善建设方案》，遵循交通气象服务使用的视频数据安全硬件配置标准和安全共享规则，明确各方权责。

（二）加强技术研发，筑牢数据闭环流转防护体系。在交通执法局、交管总队、公服中心专网之间部署边界安全设备、硬件防火墙，建设专线实现跨部门数据可控交互，全网落实等级保护建设；运用图像压缩降质、数据脱敏技术，规避敏感个人信息泄露风险；部署数字水印溯源技术，实现数据来源操作可查；统一多源异构数据采集、传输、存储技术标准，实现数据应用全链条闭环安全管理，保障内部数据规范有序流转。

（三）搭建协同应用系统，实现数据产品安全供给。气信公司搭建省级高速公路恶劣气象条件监测预警系统，打通跨部门业务与数据链路。集成统一身份认证、分级权限管控等核心安全技术，实现全域用户、全业务行为统一管理；依托专网 API、系统插件等交

互方式，仅传输加工后的气象服务产品；横向对接交通运输、公安交管等部门业务平台，实现产品联动下发，构建数据安全共享、业务联动处置的闭环应用体系，提升恶劣天气交通应急处置能力。

三、典型意义和安全治理成效

通过落实数据统一管理、全流程技术防护、跨部门闭环流转等安全治理措施，建成合规可控的交通气象数据治理体系。依托安全治理赋能交通数据融合应用，全省高速恶劣天气风险防控能力持续增强，预警服务覆盖全省200余家业务单位、2000余名一线责任人，显著降低因恶劣天气导致的经济损失，充分体现数据安全治理的实战效能与综合价值。

基于气象数据跨平台交易场景的数据流通安全技术应用案例

一、数据流通场景和安全治理挑战

在推进气象数据要素市场化配置改革过程中，存在跨平台数据流转难、流通机制不畅等挑战，福建省气象服务中心（以下简称“服务中心”）联合福建省数据流通控股有限公司，依托福建大数据交易平台（以下简称“交易平台”）共建“福建气象数据专区”，推动气象数据跨平台安全共享与开放流通。

该案例场景中的业务流程为，服务中心对拟流通数据产品进行权属确认并做流通交易登记备案；同时作为气象数据提供方将数据产品于交易平台上架，通过福建气象数据服务中台（以下简称“数据中台”）对气象数据进行服务化加工，形成标准化服务接口。数据需求方通过交易平台实名认证后可浏览并订购气象数据产品。数据供需双方通过交易平台完成服务合同与数据共享协议的签订并实现线下交付。

上述场景中存在安全治理挑战，随着跨平台流通渠道拓宽，多方协作存在权责边界模糊、交易平台易留存数据以及全过程安全风险监管难等痛点，导致气象数据易被窃取和外泄。

二、安全治理措施

（一）通过明权责和定标准保障数据“零存储”流转。供需双

方与交易平台签订三方数据服务协议，厘清各方在数据供给、流通服务、应用使用的权责。服务中心严格执行“数据来源合规审核”前置机制，确保产品合规上架，以标准化接口提供加工数据服务接口，交易平台仅做安全路由接口转发，实现线上服务、线上交付，确保数据“过路不留存”。数据需求方签署气象数据安全共享相关协议，以法律契约形式明确安全义务。

（二）多重防线实现数据“服务化交付”与“受控访问”。依托数据中台构建“产品授权—多重校验—访问管控”分层防线。将原始气象数据转化为数据服务产品，需求方仅能获取加工后的气象产品，不接触原始数据。同时，服务接口实行“按需获取”，采用动态时效令牌认证实现“一产品、一编码、一授权”，为数据需求方分配唯一且需定期申请的令牌；并将“用户认证与数据获取”“数据清单与数据下载”等核心环节解耦；结合 IP 白名单、限流封禁、细粒度权限、访问时效等策略，实现数据可用可控。

（三）建立自动化联防联控机制保障安全事件快速响应。构建供给联动安全监控体系，服务中心负责源端策略，交易平台负责流量监控。建立“监测—预警—熔断”自动化闭环，一旦检测到高频爬取等高风险行为，立即自动切断连接并冻结权限，无需人工干预即可阻断风险。同时，基于全量日志建立常态化审计，确保流通过程“行为可查、责任可究、风险可控”。

三、典型意义和安全治理成效

服务中心依规开展气象数据备案审批等规范流程，形成 38 款

高适配、易流通的气象服务数据产品，有效破解气象数据流通应用壁垒。同时，联合福建省数据流通控股公司搭建“制度定责+技术控险+监督闭环”综合治理架构，形成气象数据“广域流通、安全直达”的跨平台安全流通渠道。该模式精准化解多方协作权责不清、监管薄弱等安全短板，精简数据流通与交易服务环节，实现数据交付流程可控、可溯源；截至2026年5月，累计监测数据访问量达569万次，进一步畅通气象数据要素市场化交易渠道，充分释放气象数据要素价值，实现流通效能与安全防护双向提质增效，为气象数据共享流通安全管理提供实践参考。

基于风电场站吊装作业场景的气象数据流通安全应用案例

一、数据流通场景和安全治理挑战

内蒙古自治区是我国重要能源战略基地，风电场站建设高速发展。风机吊装属高危高空作业，对突发大风、阵风等气象条件极为敏感。针对气象数据在安全合规前提下高效流通问题，内蒙古自治区气象数据中心联合赤峰市气象局研发“气象数据融合应用服务支撑平台”（简称“气象通”），构建面向风电场站吊装场景的气象数据安全流通服务，赋能能源气象服务安全应用。

该案例场景中的业务流程为，气象部门作为数据提供与加工方，在气象专网内汇聚多源观测与预报数据，并加工制作吊装作业气象监测预报预警专项服务产品。经脱敏聚合后的产品，通过“气象通”平台单向同步至互联网隔离区。风电场站施工企业作为数据需求方，通过部署于现场的专用终端获取场景化数据产品。

上述场景中存在安全治理挑战，一是原始数据服务模式存在脱离管控、无限制复制传播甚至篡改风险，数据源头安全面临考验；二是数据产品跨专网、隔离区至用户端流转，传输链路长，存在违规调用风险；三是野外作业现场环境复杂，终端管控难度高，数据在用户端易被私自留存或越权访问。

二、安全治理措施

（一）构建分级加工体系，确保数据源头安全。建立“基础数据—融合数据—场景产品”三级数据分层治理机制，原始多源气象数据全量驻留气象专网，作为融合加工基座；中间层在气象专网完成时空对齐、质量控制与应用分析；面向吊装作业需求深度加工且经脱敏聚合后的场景化数据产品，进入后续流通环节。

（二）实施全链路流通管控，防止数据泄露。建立跨安全域分层管控机制，内部专网与对外服务平台之间实施数据单向流转，严防数据回流。平台间调用数据时，采用接口调用签名校验与动态令牌授权技术，限定调用频次与范围，防范恶意爬取；面向终端用户交付产品时，按场景实行数据资源逻辑隔离与最小权限分配，杜绝超范围访问与横向越权。

（三）建立终端数据交付管控，实现“可用不可见”。通过专用设备与业务场景绑定认证，对终端身份进行加密校验，结合动态口令机制确保接入身份真实可信、通信链路安全可靠。终端交付环节遵循数据最小化展示原则，仅提供业务决策所需场景化数据产品可视化服务，不提供原始数据留存或导出功能，形成终端安全闭环。

三、典型意义和安全治理成效

案例立足内蒙古风电场站吊装作业场景，破解气象数据跨网域安全流通服务难题，构建“分级加工、通道防护、终端管控”的全链路安全流通服务模式，为气象数据产品向能源行业合规流通提供了可复制、可推广的实践样板。通过上述措施，实现气象数据产品从专网加工到现场应用的全链路安全管控，数据泄露、篡改、滥用

等安全事件零发生。案例服务覆盖内蒙古7个风电场站400余台风机，有效提升数据供给效率、作业决策精准度与安全生产能力，对全国风电场站密集区域的气象数据安全流通服务具有推广示范作用。

基于气象数据滥用防范场景的数字信封安全技术应用案例

一、数据流通场景和安全治理挑战

随着气象数据要素市场化配置改革工作推进，气象数据跨领域流通应用快速增长，数据传输过程中易被截获、跨项目滥用难管控等问题日益突出，以防火墙为代表的传统边界防护策略，难以解决数据出域后的安全可控问题。广东省气象服务中心作为广东气象数据授权运营主体，构建端到端数字信封保护机制，支撑气象数据安全受控流通。

该案例场景中的业务流程为，广州数据交易所建设气象服务产品专区并开展供需撮合，广东省气象服务中心作为数据提供方，向数字广东公司承建的广东省应急指挥业务系统提供13项气象数据组件产品。数据产品以组件化方式交付，采用一项目一授权模式，通过授权调用嵌入业务系统，实现气象数据从产品加工、挂牌交易到场景应用的闭环流通。

上述场景中存在安全治理挑战，一是气象数据授权运营审核规则在操作层面的标准化、模板化、清单化程度不够，审核执行口径尚未统一；二是数据跨域流通过程中缺乏有效保护机制，数据多以明文接口形式提供，存在被抓取和复制滥用风险；三是数据产品集成应用环节缺乏约束与监管机制，组件跨项目使用存在超范围调用

和滥用风险。

二、安全治理措施

（一）建立气象数据授权运营的审核规范。依据国家层面《中华人民共和国数据安全法》《中华人民共和国气象法》和气象行业《非涉密气象数据资源分类分级指南（试行）》《公共气象数据授权运营管理办法（试行）》等法律法规，建立气象数据授权运营的审核规范。对流通数据实行数据产品分类分级认定、气象数字身份标识申领和流通合规审核。坚持数据产品“先审核后流通”原则，为气象数据要素合规流通提供制度保障和治理基础。

（二）构建端到端数字信封的保护机制。遵循自主可控的商用密码国家标准，构建“后端中台动态加密+前端组件容器内解密”的端到端数字信封保护机制。SM2 算法负责封装会话密钥、SM3 算法负责保障数据完整性、SM4 算法负责加密业务数据。坚持“数据可用不可见”原则，不提供明文接口，不允许原始数据脱离组件环境使用，防范链路截获、非法缓存和二次复制风险，推动气象数据由传统边界防护向数据加密受控保护转变，有效防范数据滥用风险。

（三）实现一项目一授权的监管闭环。坚持一项目一授权原则，将前端组件使用权限与具体合同、应用场景及有效期绑定，未经重新授权不得迁移复用，从机制上防范跨项目调用和超范围使用。通过记录主体身份、授权项目运行环境约束条件、调用频次等事件日志，并以此为基础通过自动化监测机制实时识别并报告恶意爬取等

安全事件；执行日志防篡改保护，确保审计证据真实性与不可逆，为验证应用场景与授权合约的一致性提供动态监控和审计存证。通过技术控制与运营监管协同联动，实现数据产品流通全过程可管可控的闭环治理。

三、典型意义和安全治理成效

该案例以数字广东公司采购在广州数据交易所挂牌的13项气象数据组件产品，并嵌入广东省应急指挥业务系统为典型应用场景，通过气象数据授权运营审核规范、端到端数字信封保护机制和一项目一授权监管闭环，有效防范数据截获、跨项目滥用和二次转售风险，实现了气象数据由传统接口供给向安全受控交付转变。该案例为气象数据产品安全流通提供实践参考，对气象数据规模化流通具有示范推广价值。

基于三峡防洪和水电调度场景的气象数据流通安全应用案例

一、数据流通场景和安全治理挑战

在三峡梯级水库防洪、水电调度场景中，气象数据存在跨行业协同不畅、跨网域流通安全防护不足、分类分级管控精细化不够等突出问题。为此，湖北省气象信息与技术保障中心联合三家单位，健全协同管控机制，强化技术防护能力，落实分类分级要求，依托气象数商服务平台和气象数据流通监管平台，构建多方协同气象数据流通安全应用体系，推动数据合规流通与价值释放。

该案例场景中的业务流程为，湖北省气象信息与技术保障中心为数据提供方和平台建设方，负责汇聚库区及受电区域多源气象数据、开展数据治理与安全监管，并提供平台支撑；湖北省气象台、气候中心为数据加工方，负责数据融合、模型训练及定制化气象服务产品制作；三峡水利枢纽梯级调度通信中心为数据需求方，获取气象数据并应用于梯级调度。

上述场景中存在安全治理挑战，一是气象与水电行业数据标准、接口不统一，权责划分模糊，协同效率低；二是气象专网与三峡调度专网架构、安全策略差异大，数据跨网传输易受攻击，现有管控溯源技术难以兼顾安全与时效；三是气象数据类型繁杂，行业分级标准不完善。

二、安全治理措施

（一）健全协同管控机制，明确权责与合规底线。依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规及行业规范，明确多方协同单位的权责边界，签订数据安全协议；统一数据格式与接口规范，遵循数据流通安全原则，建立“最小授权+动态管控”的访问机制，实行“最小范围”授权。同时，建立动态权限调整机制，明确授权主体、审批流程及有效期，对异常访问实时告警阻断，将安全合规行为与数据服务优先级、合作评价挂钩，形成正向激励。

（二）强化技术防护能力，破解跨网流通安全难题。按“一内一外”定位建设气象算力设施：对内建成气象数据云算力设施，对外建成共享算力设施；建设气象数商服务平台，提供标准化访问接入服务；运用气象数字身份标识技术实现数据全生命周期标识管理与溯源；配备态势感知、数据加密等安全软件，应用 IP 白名单、流量限流等防护措施，相关系统完成等保三级备案及测评。

（三）落实分类分级要求，实施与业务场景深度适配的管控措施。严格落实国家数据分类分级保护制度，结合气象行业标准和业务特点将气象数据划分为不同级别。根据数据级别匹配差异化访问权限、安全策略和技术措施，依托两大平台规范流通流程、留存操作日志，实现安全与效率平衡。

三、典型意义和安全治理成效

本案例立足三峡防洪和水电调度核心场景，有效破解了气象数

据跨行业、跨网域流通难题，构建“机制健全、技术先进、生态完善”的安全治理模式。通过上述措施，实现气象数据流通安全管控，可有效拦截违规访问，数据泄露、篡改等安全事件零发生；三峡梯级电站水资源利用率显著提升，有效防范气象灾害风险。同时，提升了数据供给效率与调度精准度，为重大水利工程气象数据流通提供示范引领。