

《低空经济 信息服务系统数据安全技术要求》

（征求意见稿）

编制说明

一、工作简况

（一）任务来源

本标准由广东工业大学提出，经中国技术市场协会批准，正式列入 2025 年团体标准制修订计划，标准名称为《低空经济 信息服务系统数据安全技术要求》。

（二）项目背景

随着低空空域管理改革的推进及低空经济的快速发展，无人机、eVTOL、电动轻型飞行器等低空飞行器广泛应用于物流运输、巡检监测、应急救援、航空摄影等多个领域，推动低空空域逐步开放。与此同时，低空信息服务系统在飞行计划申请、动态监控、交通管理、气象播报、地理信息等方面发挥关键作用。其核心依赖于大量高频次、多维度、跨系统的数据交换与协同处理。

然而，低空信息服务系统在建设和运行中正面临日益突出的数据安全挑战，主要表现为：首先，飞行器识别、轨迹、控制指令等关键数据被篡改或泄露，可能引发飞行事故甚至社会安全风险；其次，服务平台与用户、监管系统之间的接口通信未加密或无访问控制，存在数据劫持或非法注入的隐患；最后，缺乏统一的数据权限分级管理与行为审计机制，易造成数据滥用或责任难以追溯。

（三）目的意义

制定标准的目的与意义在于：第一，构建系统层级的安全防

护基础框架，明确在系统架构设计中应遵循的数据安全控制技术规范；第二，全面提升行业在数据安全方面的综合保障能力，有效防控因人为误操作或恶意攻击所引发的系统运行中断及敏感信息泄露风险；第三，为监管机构与运营主体提供统一、可执行的安全管理依据，促进低空经济的安全、有序与可持续发展；第四，支撑国家空域管理体系的数字化转型战略，推动《网络安全法》《数据安全法》等相关法律法规在低空领域的规范化贯彻与实质性落地。

（四）起草单位及起草人名单

本标准起草单位：×××××××、×××××××、×××××××等。

本标准主要起草人：×××、×××、×××、×××、×××、×××等。

（五）主要起草过程

1. 文本调研

2025 年 4 月启动了文本的调研工作，并与 2025 年 5 月完成了相关资料的收集和分析工作。

2. 标准立项

广东工业大学向中国技术市场协会提出申请，于 2025 年 5 月获得中国技术市场协会批准立项。

3. 组建标准起草工作组

2025 年 9 月 16 日，召开项目启动会。

2025 年 9 月 17 日，成立了标准起草工作组，并讨论标准调研工作事项。

4. 形成标准草案

2025 年 10 月 9 日，起草组对资料收集情况进行汇报，并对进行了线上讨论。

2025 年 10 月 10 日，开展组内讨论，确定了标准框架和主要内容。

2025 年 10 月 10 日，对广东工业大学起草的标准初稿进行现场讨论，并提出修改意见。

2026 年 10 月 20 日，起草组根据修改意见进行修改，形成标准草案。

5. 形成征求意见稿

2026 年 10 月 26 日，对标准草案进行讨论，起草组对草案内容进行了修改，形成标准征求意见稿。

二、确定标准主要内容的论据

（一）编制原则

本标准按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》以及《中国技术市场协会团体标准工作程序》的规定起草。

（二）标准主要内容及适用范围

本标准规定了低空信息服务系统（以下简称“低空系统”）进行数据收集、传输、存储、使用、提供、删除等数据处理活动的安全技术要求。

本标准适用于低空系统进行数据处理活动中的数据安全管理工作。

（三）确定标准主要内容的论据

本标准重点规范如下内容的技术要求：数据分类分级与访问控制，数据加密与链路保护，身份认证与授权机制，数据完整性与防篡改要求，安全审计与日志管理，以及数据安全事件响应与恢复机制。基于 2025 年低空经济发展现状与技术趋势，结合案例数据，阐述本标准主要内容的论据：

首先，本标准的分类分级机制是基于 2024 年多起无人机劫持事件教训编制，通过数据分类分级，并匹配差异化防护措施，满足《数据安全法》第 21 条对重要数据目录的要求。

其次，针对低空链路攻击高发，本标准提出的数据加密内容，可以降低攻击率，为密钥需芯片硬件管理规定提供支持，既符合工信部 2025 年设备准入清单的国产化要求，又可保障跨平台数据交换的防护有效性。

再次，标准设定身份认证与授权机制、数据完整性与防篡改和事件响应与恢复机制的内容，是为了应对 2025 年"虹膜伪造 2.0"技术导致的生物认证风险和 2024 年无人机劫持事件教训。本标准的内容可以兼顾低空经济信息系统服务数据的安全性与业务灵活性，通过安全审计与日志管理，满足监管合规性，又显著降低了传统人工审计成本。

三、主要试验[或验证]情况分析、技术经济论证、预期经济效果

本标准制定具有重要的社会效益，主要包括：

（1）建立系统级安全防护基线，规范系统架构设计中的数据安全控制要求。本标准已经在深圳、海南等低空改革试验区开展压力测试，重点验证跨境数据流动管控模块。其中，在模拟低

空异构网络环境中，验证数据分级分类控制模块的可靠性，可以实现飞行轨迹、用户身份等敏感数据与其他数据隔离传输，使得误判率控制在 0.01%以内。

（2）提升行业数据保护能力，减少人为误操作和恶意攻击引发的系统瘫痪或信息泄漏。按照成本-收益模型对此标准的提出进行论证可知，采用低空经济信息服务系统数据安全标准，需要前期投入的成本包括确保技术实施的单套系统加密模块升级费用、流程改造费用和接口标准化改造成本，其对应可获得的收益内容包括了数据泄露损失降低、监管处罚规避和数据共享效率提升等内容。在此情况下，如果沿用传统航空标准，例如沿用 DO-326A 航空安全框架时，需额外增加 22%的低空场景定制化开发成本；另外，本标准针对 200 米以下空域优化，在符合 ISO/SAE 21434 的自动驾驶数据安全要求的前提下，可以降低 18%的能耗。

（3）为监管与运营平台提供安全准则，推动低空经济健康可持续发展。支持国家空域管理数字化转型，落实《网络安全法》《数据安全法》等法律法规在低空领域的延伸落地。通过标准化数据接口，空域审批时间从 72 小时压缩至 8 小时，促进城市空中交通（UAM）商业化进程。构建《数据安全法》在低空领域的实施细则，填补 400 米以下空域数据主权管理空白。为智慧城市低空管控系统提供安全数据底座，支撑全国 2800+县区的空域资源动态调度。具体地，根据 2025 年低空经济白皮书及工信部试点监测报告推算，未来 5 年期间，因本标准的实施可减少的低空经济数据事故损失将达年度产业规模的 0.8%-1.2%。

四、采用国际标准和国内外先进标准的程度

本标准为首自主制定，本标准不涉及国际国外标准的采标情况。

五、重大分歧意见处理经过及依据

本标准在制定过程中未出现重大分歧意见。

六、与现行相关法律、法规及相关标准的协调性

本标准符合国家现行法律、法规和强制性国家标准的要求，参考了 GB/T 17901 信息技术安全技术 密钥管理、GB/T 20988 信息技术安全技术 信息系统灾难恢复规范、GB/T 31500 信息安全技术 存储介质数据恢复服务要求、GB/T 31509 信息安全技术 数据安全风险评估实施指南、GB/T 35273 信息安全技术 个人信息安全规范、GB/T 37988 信息安全技术 数据安全能力成熟度模型、GB/T 39335 信息安全技术 个人信息安全影响评估指南、GB/T 41479 信息安全技术 网络数据处理安全要求、GB/T 43697 数据安全技术 数据分类分级规则等国家标准相关内容要求。

七、知识产权情况说明

本标准不涉及知识产权。

八、其他应予说明的事项

无。

《低空经济 信息服务系统数据安全技术要求》

团体标准起草组

2025 年 10 月 26 日