ICS 03.220.50
CCS V54

T

团　　体　　标　　准

T/TMAC ×××—202X

低空经济 信息服务系统数据安全技术要求

Low-altitude economy——Technical requirements for data security in information service systems

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

××××-××-××发布　　××××-××-××实施

中国技术市场协会　　发布

中国技术市场协会（TMAC）是科技领域内国家一级社团，以宣传和促进科技创新，推动科技成果转移转化，规范交易行为，维护技术市场运行秩序为使命。为满足市场需要，做大做强科技服务业，依据《中华人民共和国标准化法》《团体标准管理规定》，中国技术市场协会有序开展标准化工作。本团体成员和相关领域组织及个人均可提出制修订 TMAC 标准的建议并参与有关工作。TMAC 标准按《中国技术市场协会团体标准管理办法》《中国技术市场协会团体标准工作程序》制定和管理。TMAC 标准草案经向社会公开征求意见，并得到参加审定会议多数专家、成员的同意，方可予以发布。

在本文件实施过程中，如发现需要修改或补充之处，请将意见和有关资料反馈至中国技术市场协会，以便修订时参考。

中国技术市场协会地址：北京市海淀区复兴路甲 23 号城乡华懋大厦 12 层 1217 室。

邮政编码：100036　　电话：010-68270447　　传真：010-68270453

网址：www.ctm.org.cn　　电子信箱：136162004@qq.com

目　次

前　言

本文件按照 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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东工业大学提出。

本文件由中国技术市场协会归口。

本文件起草单位：广东工业大学、××××××××××××。

本文件主要起草人：赵佳虹、潘晓杰、张龙飞、柯紫琪、傅惠、×××、×××、×××、×××、×××、×××。

低空经济 信息服务系统数据安全技术要求

1 范围

本文件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。

本文件适用于低空系统进行数据处理活动中的数据安全管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 17901 信息技术安全技术 密钥管理
GB/T 20988 信息安全技术 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

3 术语和定义

GB/T 17901、GB/T 20988、GB/T 31500、GB/T 35273、GB/T 37988、GB/T 41479 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CA：证书颁发机构（Certificate Authority）
CRC：循环冗余校验（Cyclic Redundancy Check）
ETL：采集，转换，加载（Extract, Transform, Load）
TLS：传输层安全（Transport Layer Security）
SHA：安全哈希算法（Secure Hash Algorithm）

5 一般要求

低空系统在数据采集、传输、处理、存储和共享等全过程中，应确保数据安全管理制度的健全性、技术措施的充分性和保护措施的有效性。一般要求如下：

a) 数据处理活动应符合 GB/T 41479 规定，建立覆盖数据生命周期的管理控制机制，确保数据的保密性、完整性和可用性；
b) 涉及个人信息的处理活动，应符合 GB/T 35273 提出的原则和要求，包括最小必要、明示告知、目的限定、主体权利保障等内容；
c) 应依据 GB/T 43697，开展数据分类分级工作。应明确区分核心数据（含航空器实时动态航行数据、飞行控制指令、空域管制核心指令、系统核心配置数据等，泄露或破坏将直接威胁低空航行安全或造成重大影响）、重要数据（含用户实名身份信息、飞行计划数据、航空器登记信息、飞行轨迹历史数据、系统安全日志等，泄露或破坏将导致用户权益受损或较大范围影响）、一般数据（含公开空域基础信息、公开气象信息、系统公开服务说明等，具有公开性，泄露影响较小），制定与数据等级相匹配的保护策略、访问控制措施及审计机制；
d) 应结合低空航行服务业务特征，识别涉及的一般个人信息与敏感个人信息（如位置信息、身份

信息、行为轨迹等），并依据 GB/T 35273 中的定义进行标识、分级管理与脱敏处理；

e) 系统整体数据安全保障能力应至少达到 GB/T 37988 中定义的第 2 级能力要求，即建立了基本制度流程，具备初步风险识别、控制和响应能力；

f) 数据处理单位应根据 GB/T 31509，结合自身系统结构、业务流程及数据种类，定期开展数据安全风险评估，评估周期不应超过 12 个月，或在系统重要变更后即时开展；

g) 对于可能对个人权益产生重大影响的个人信息处理活动（如位置追踪、画像分析、自动决策等），应在处理前依据 GB/T 39335 开展个人信息保护影响评估，并形成书面报告，明确风险源、影响对象、缓解措施及责任分工；

h) 评估报告、分类分级结果和保护策略应完整归档，并接受监管部门抽查或审计时调阅。

6 数据收集

6.1 通则

低空系统在提供低空航行信息服务过程中，应严格控制数据采集范围、频率和权限，确保数据收集合法、正当、必要，保障用户的个人信息权益。数据收集的基本要求包括告知同意、范围最小化、权限最小化三个方面。

6.2 告知同意

低空系统在开展个人信息收集前，应依据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》以及 GB/T 35273《个人信息安全规范》、GB/T 41479《网络数据处理安全要求》、GB/T 39335《个人信息安全影响评估指南》等相关标准的要求，遵循合法、正当、必要原则，落实信息主体知情权与同意权，具体包括：

a) 在用户使用航行信息服务申请、计划报备等功能前，应通过显著方式以清晰、易懂的语言向用户告知以下内容：

——平台或系统的名称、运营主体及联系方式；

——个人信息处理的目的、方式（如本地处理、云端存储、数据共享等）；

——收集的个人信息种类（如姓名、身份证件号码、联系方式、飞行计划、历史轨迹等）；

——信息的保存期限及到期后处理方式；

——用户行使其查询、更正、删除、撤回同意、投诉举报等权利的路径与方式。

b) 在完成上述信息充分告知后，应取得用户的明示同意，并通过可验证的方式予以记录和保存，如点击确认、电子签名等方式，确保同意过程的可溯源性。

c) 对于涉及实名认证的场景，应依据 GB/T 35273 的规定，向用户说明实名认证的法律依据与实现目的的必要性，严格遵循最小必要原则，所收集的身份信息仅限于完成认证所必需的内容。

6.3 收集范围

低空系统应依据 GB/T 41479、GB/T 35273 和 GB/T 43697 要求，遵循最小必要原则进行数据收集，其数据范围应满足以下要求：

a) 所收集的数据应与航行服务直接相关，且为实现服务所必需的信息，不得超范围采集；

b) 收集个人信息的种类、数量和敏感程度应与所提供业务功能之间存在直接关联；

c) 应对数据采集活动的时间、地点、对象、内容、方式等进行系统日志记录，并保存备查，以支持数据溯源和行为审计，宜参照 GB/T 31509；

d) 自动采集的数据频率应为实现业务功能所必需的最低采样频率，避免过度采集；

e) 涉及敏感个人信息的场景，应根据 GB/T 39335 进行个人信息影响评估，并保留评估文档与结论。

6.4 权限范围

低空系统在移动终端或其他操作系统中运行时，其所申请的系统权限应满足以下要求：

a) 在设计阶段依据 GB/T 41479 明确系统权限清单，并在用户授权前以清晰、完整、易理解的方式公开声明各权限的名称、用途及必要性；

b) 所申请的操作系统权限应限于实现核心业务功能所必需，且不得申请与数据收集无关或与服务功能无关的权限；
c) 应建立权限访问控制与行为日志机制，确保权限调用行为具备可追溯性（参考 GB/T 37988 中关于访问控制的能力等级要求）；
d) 权限策略变更前（如新增高敏权限）应再次取得用户授权并更新日志。

7 数据传输

7.1 保密性

低空系统传输数据时应在满足 GB/T 35273 保密要求的基础上，遵守以下保密性控制措施：
a) 应采用符合国际标准的数据加密协议建立通信通道，例如 TLS 1.3 及以上版本、IPSec、DTLS 等，确保数据传输过程中不被窃听、仿冒或重放；
b) 向外部系统（如监管平台、气象服务系统等）传输数据时，应明确数据共享范围与加密策略，通过签订协议或策略清单形式约定双方的加密方式、接口防护机制和访问控制要求；
c) 敏感数据（如实名信息、控制指令、实时轨迹）应采用端到端加密方式，在传输前加密处理，在接收端解密，确保数据在整个链路中的保密性。

7.2 可行性

低空系统应保障数据传输的可行性、连续性与恢复能力，建议采取以下措施提升传输通道的高可用性：
a) 网络架构应设计具备多路径备份能力，构建双链路、双接入或链路聚合机制，提高物理链路冗余度（参考 GB/T 20988 第 6 章“系统可用性”）；
b) 根据业务对延迟与带宽的要求，合理设计数据包大小、传输窗口、流控机制与重传机制，优化链路性能；
c) 应引入错误检测与纠正机制，如 CRC、FEC 等，以应对链路中可能出现的数据误码或丢包问题；
d) 采用负载均衡机制对网络流量进行动态分配，防止传输瓶颈和流量突发拥堵，确保关键业务实时通达；
e) 对关键链路应部署实时监测与故障告警机制，记录链路波动信息并支持系统自动切换，提升故障响应效率；
f) 针对不同类型数据的传输需求差异，建立差异化优先级调度机制，明确关键数据（如实时航行状态、控制指令）与非关键数据（如历史数据统计）的传输优先级判定标准及调度逻辑，确保核心业务数据优先传输；
g) 增强网络适应性，针对弱网、异构网络切换等场景，采用本地缓存、断点续传、数据压缩等技术保障传输连续性，同时对缓存数据实施加密保护与有效期管理，防止敏感信息泄露或数据失效；
h) 完善主备链路数据同步机制，在主链路故障恢复后，通过数据校验、时间戳比对等方式确保主备链路数据一致性，保障切换过程中数据不丢失、不重复；
i) 明确传输质量的核心指标要求，结合低空航行服务的实时性与可靠性需求，对数据传输的延迟、抖动、可用率等关键指标制定相应的保障标准。

7.3 认证可达

为确保传输数据的认证可达性、真实性、完整性与可追溯性，低空系统在传输过程中应实施数据认证与确权机制，包括：
a) 在数据传输前应完成双方的身份认证与授权过程，推荐使用基于数字证书或分布式身份体系的认证机制，确保数据来源与接收方的真实性；
b) 在数据传输过程中，应对传输数据使用哈希校验（如 SHA-256）、消息认证码等技术进行完整性验证，防止数据在传输链路中被篡改；
c) 对关键数据的传输过程应进行全程记录与同步，实现数据传输过程的不可否认性与溯源可追踪性（参考 GB/T 37988 与 GB/T 31509 风险控制建议）；

d) 建议建立传输审计日志归档策略，结合低空系统日志审计模块记录每一次数据交互行为，支持事后取证与异常行为分析。

8 数据存储

8.1 一般要求

低空系统进行数据存储时，应在满足 GB/T 35273 数据存储要求基础上，进一步遵循以下要求：

a) 对于用户的敏感个人信息（如身份证号、电话号码、位置信息等），应采用国家认可的对称/非对称加密算法（如 SM4、RSA）进行加密存储，并采取访问控制与脱敏展示等措施限制访问范围；
b) 密钥管理应遵循 GB/T 17901 中的全生命周期管理要求，包括密钥生成、存储、分发、使用、更新和销毁，并配置密钥托管与权限隔离机制；
c) 监控类数据（如系统日志、链路状态信息）应至少保存 12 个月，飞行任务数据、用户交互数据等其他重要数据应至少保存 15 个月，并确保期间数据可用性和审计完整性；
d) 加密数据的备份和恢复操作应受到保护，应通过隔离区或安全模块确保加密状态不被破坏，支持在不降低数据安全等级的前提下快速恢复服务；
e) 备份应按照 GB/T 43697 根据数据分类分级制定差异化策略，对重要或核心数据采用多介质、多位置备份，并具备介质丢失或非法访问下的自保护能力（如加密、不可读格式）；
f) 应制定数据修复与回滚机制，在数据出现错误或被破坏时，结合备份内容及恢复流程进行快速恢复，确保数据业务连续性和一致性。

8.2 备份要求

低空系统应建立完善的数据备份与恢复机制，结合 GB/T 20988 和 GB/T 31500 要求，从本地与异地冗余、多级备份频率、服务流程及恢复方式等方面落实保障：

a) 系统应支持本地实时备份与周期性异地备份，对关键数据库、飞行记录、用户交互等数据采用分层备份策略，保障在自然灾害、硬件故障等极端情况下的数据完整性；
b) 应对数据库文件、系统配置项、重要日志等数据每周进行一次完全备份，每日进行至少一次增量备份，并记录备份版本信息，支持按时间点恢复；
c) 数据恢复流程应参照 GB/T 31500 中相关要求，落实恢复服务所需的技术能力（如数据镜像、冗余节点）、服务保障（如恢复时间目标）与安全控制（如恢复后校验）；
d) 灾难恢复机制应符合 GB/T 20988 恢复资源配置与恢复实现方式要求，建设具备自动切换、应急响应和容灾演练能力的恢复系统，确保低空系统在严重故障情况下 24 小时内恢复核心功能。

9 数据使用

9.1 访问控制

低空系统对数据访问的控制应满足以下要求：

a) 对用户个人信息的访问应符合 GB/T 35273 关于访问控制的规范性要求；
b) 建立数据访问审批机制，对用户个人身份信息、电话号码、地址等敏感信息设置操作限制，防止非法批量查询和导出；
c) 涉及查看或处理敏感信息的操作（如导出身份信息），应采用与登录认证不同的二次验证机制，如短信验证、生物识别或 USB-Key；
d) 依据 GB/T 37988 最小权限原则，根据操作人员的职责角色划分访问权限，杜绝越权访问。

9.2 信息显示

低空系统在显示数据信息时，应采取数据去标识、模糊处理与审慎授权相结合的措施，满足以下要求：

a) 展示用户个人信息应满足 GB/T 35273 相关要求，不展示无关或冗余字段，避免曝光用户隐私；
b) 对飞行活动数据中涉及的申请人、操控员等自然人信息，应默认进行脱敏（如手机号脱尾、姓名部分遮蔽），如确因业务需要查看原始数据，应在界面中添加水印并记录审计日志；

c) 涉及展示敏感信息的场景，应提前依据 GB/T 39335 要求开展个人信息影响评估，并根据评估结果制定保护措施；
d) 对低空空域、低空航线、起降点/场、低空航空器位置等地理空间数据，应采用加偏、坐标网格化、模糊算法等方式在不影响服务精度的前提下减少泄露风险。

9.3 导出数据

低空系统进行数据导出时，应实施严格的身份校验与导出过程控制，满足以下要求：
a) 对导出操作设置明确的权限控制策略，仅授权用户可进行数据导出操作，并记录操作时间、内容、目标等信息；
b) 对批量导出敏感数据（如身份信息、家庭住址、电话号码等）进行严格监控，建立行为日志与异常告警机制；
c) 导出敏感个人数据前应通过认证核验导出人的身份，防止内外部攻击者滥用导出功能；
d) 对导出后的数据文件应加密处理，设置下载时效与自动销毁机制。

9.4 记录日志

低空系统应在数据使用全过程中进行详尽的日志记录与保护，符合 GB/T 31509、GB/T 20988 等标准要求，具体如下：
a) 低空系统的日志类型包括但不限于：
   1) 低空系统日志：记录系统运行状态、错误与异常；
   2) 低空系统安全日志：记录身份认证、访问控制、安全事件；
   3) 低空系统访问日志：记录资源访问详情，如 IP 地址、端口、会话时长、访问接口等。
b) 低空系统日志应满足：
   1) 全面记录事件细节，含时间戳、事件类型、操作用户、资源对象等；
   2) 时间同步精度不低于毫秒级，用户标识与行为一致；
   3) 日志格式标准统一，支持集中采集与分析；
   4) 日志一旦生成应加密存储并具备防修改、防删除能力。
c) 低空系统日志保存期限应符合隐私保护与业务要求，一般不应少于 12 个月，对涉及安全事件的日志应延长保存期限。
d) 低空系统日志安全保护措施应包括：
   1) 依据岗位设置访问权限，访问敏感日志需二次验证，定期审计权限有效性；
   2) 敏感操作如删除或修改日志应通过审批流程并记录操作人员信息，日志数据应加密或签名保护；
   3) 定期执行全量与增量备份，设置周期性备份任务，支持日志灾难恢复和取证需求。

10 数据删除

10.1 删除范围与时机

应明确需要删除的数据类型，包括但不限于：过期的用户个人信息（如身份信息、位置轨迹）、失效的飞行任务数据、冗余备份文件、废弃系统存储介质中的数据等；

数据删除的时机应满足：
a) 符合法律法规或服务协议约定的保存期限（如个人信息保存期满且无留存必要）；
b) 用户主动申请删除个人信息并经核验通过后；
c) 系统终止服务或存储介质废弃前；
d) 经数据安全风险评估认定为高风险且无需留存的数据。

10.2 删除技术要求

针对不同存储场景和数据敏感性，采用以下删除方式，确保数据无法被非法恢复：
a) 逻辑删除：适用于需暂时隐藏但可能需回溯的数据（如用户注销后暂存的历史记录），通过数据库标记（如设置“删除标识”字段）或文件系统索引移除实现，使数据在常规访问中不可见；

逻辑删除后，需限制对标记数据的访问权限（仅授权审计人员可查询），且在满足彻底删除条件（如超过回溯期限）后自动触发物理删除。

b) 物理擦除：适用于电子存储介质（如硬盘、SSD、U 盘）中需彻底清除的数据（如敏感身份信息、实时轨迹），具体包括：
   1） 磁介质（如机械硬盘）：采用多次覆写技术，或通过专业工具执行低级格式化，破坏数据磁道结构；
   2） 固态存储介质（SSD）：利用固件指令执行“安全擦除”（符合 ATA 标准），清除闪存芯片中的数据块，防止通过磨损均衡机制恢复；
   3） 移动存储设备：在脱离系统前，通过加密擦除工具对全介质数据进行加密覆盖，确保无法通过数据恢复软件还原。

c) 介质销毁：适用于废弃或高敏感存储介质（如包含核心数据的硬盘、纸质档案），包括：
   1） 电子介质：对报废硬盘、芯片采用物理粉碎（颗粒度不大于 2mm×2mm）或高温熔炼，彻底破坏存储载体；
   2） 纸质载体：对打印的身份信息、飞行计划等文档，采用十字交叉粉碎（粉碎后无法拼接）或焚烧处理，确保信息完全灭失。

d) 云端数据删除：向云服务提供商发起删除指令时，需明确要求执行“彻底删除”（非逻辑删除），包括：
   1） 删除对象存储中的数据文件及冗余副本（如分布式存储的多节点备份）；
   2） 要求云服务商提供删除回执，包含删除时间、存储节点、操作人等信息，并通过技术验证（如接口查询确认数据不可访问）；
   3） 对加密存储的云端数据，同步销毁本地管理的解密密钥（符合 GB/T 17901 密钥销毁要求），实现数据不可读。

10.3 删除过程控制

数据删除前应通过审批流程，记录待删除数据的类型、数量、存储位置及删除原因，经数据安全负责人签字确认。

删除过程需全程记录日志，内容包括：删除时间、方式（如逻辑删除 / 物理擦除）、操作人员、使用工具、删除结果等，日志应加密存储且不可篡改（符合 9.4“日志记录”要求）。

删除后需进行有效性验证：

a）逻辑删除：检查数据库查询结果，确认标记数据不可见；

b）物理擦除：通过数据恢复工具扫描存储介质，验证目标数据无法被读取；

c）介质销毁：留存销毁前后的载体照片、监销人员签字记录，作为验证凭证。

验证结果与删除记录合并形成《数据删除报告》，归档保存至少 3 年，以备审计。

11 数据接口

低空系统在数据共享、交换与提供过程中，应依据 GB/T 41479、GB/T 43697、GB/T 35273、GB/T 31509、GB/T 37988 等标准建立可控、安全的数据接口，接口应部署以下控制措施：

a) 明确数据接口可共享内容与交换对象，严格限定交换数据的内容范围，仅在提供服务所需的最小范围内进行数据共享（与 6.2“收集范围最小化”一致），防止不相关系统获取无关数据（参考 GB/T 41479 与 GB/T 43697 分类控制原则）；

b) 在部署接口前，应完成接入方的身份认证与访问授权，推荐使用可信身份认证手段，如 API Key、OAuth 2.0、双向数字证书、软硬件令牌等方式核验访问者合法性；

c) 数据在共享传输过程中的机密性与完整性应通过加密通信（采用 TLS 1.3 及以上版本、IPSec 等，与 7.1a）一致）、数字签名、传输加密通道、可信时间戳等方式进行保障；对标记为“重要数据”“敏感数据”的内容应优先使用国密算法加密（与 7.1c）端到端加密要求匹配）；

d) 低空系统内部子模块间也应建立接口，使用专有协议、私有链路传输，并进行数据访问白名单限制、完整性校验与内容安全检测。

e) 对于 API、数据库访问、消息队列、FTP/HTTP 等接口形式，系统应实现统一身份认证、权限控制（与 9.1 访问控制策略一致）、速率限制、防止 SQL 注入等安全能力；

f) 接口应接入统一接口网关，具备访问异常监测功能，支持对暴力请求、爬虫行为、接口探测等

攻击行为进行识别与阻断；

g) 实现接口调用的全生命周期监控，包括访问来源、传输数据量、调用频率、失败率等，记录内容应满足 9.4 “记录日志”的要求（参照 GB/T 31509 日志管理）；

h) 应部署接口防重机制，防止接口遭受重复提交、数据采集类攻击，保障接口调用的幂等性与安全性；

i) 个人信息删除应符合 GB/T 35273 规定，包括用户主动删除请求、服务协议终止或保存期满等场景，采取物理覆盖或加密销毁等技术手段保证数据无法还原；

j) 删除操作应形成记录，包括删除数据的类型、删除方式（如逻辑删除、物理擦除）、时间、操作者及审批记录等元数据，记录需符合 9.4“日志记录防篡改、可追溯”要求；

k) 涉及重要信息系统数据删除操作应参照 GB/T 20988 和 GB/T 31500 要求纳入系统灾难恢复与数据恢复机制中，确保误删或非法删除后具备回滚能力。

参 考 文 献

[1] GB/T 38152　无人驾驶航空器系统术语

[2] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[3] GB/T 43697—2024 数据安全技术 数据分类分级规则

[4] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[5] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[6] GB/T 31509—2015 信息安全技术 数据安全风险评估实施指南

[7] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

[8] GB/T 31500—2024 信息安全技术 存储介质数据恢复服务要求

[9] GB/T 17901—2008 信息安全技术 密钥管理规范

[10] 《中华人民共和国网络安全法》

[11] 《中华人民共和国数据安全法》