ICS 03.220.50
CCS V 54

MH

中华人民共和国民用航空行业标准

MH/T 4064—2026

民用无人驾驶航空器航行服务系统数据安全技术要求

Technical requirements for data security of civil unmanned aircraft air navigation service system

2026-01-11 发布　　2026-02-01 实施

中国民用航空局　发布

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。

本文件由中国民航局空管行业管理办公室提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民用航空总局第二研究所、中国民用航空局信息中心、深圳市大疆创新科技有限公司、深圳美团低空物流科技有限公司、粤港澳大湾区数字经济研究院（福田）、浙大城市学院滨江创新中心、珠海安擎科技有限公司、中移（成都）信息通信科技有限公司、工业和信息化部电子第五研究所(中国赛宝实验室)、星控数智科技（重庆）有限公司、青岛云世纪信息科技有限公司、中国民航大学、西安交通大学、北京航空航天大学。

本文件起草人：邹翔、唐滔、杨非、孙立超、陈明、贾佳、车海翔、刘莹、耿增显、杨泽渊、陈涛、王兆星、杨亮亮、张亮、刘欢、周小霞、胡鹏、党先举、王剑飞、苏州、周剑、谢拥军、刘怡良、秦正。

民用无人驾驶航空器航行服务系统数据安全技术要求

1 范围

本文件确立了民用无人驾驶航空器航行服务系统（以下简称“USS系统”）的业务组成和数据分类，并规定了USS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。

本文件适用于民用无人驾驶航空器航行服务提供方进行USS系统数据处理活动的数据安全管理。

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—2007 信息安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 31500—2024 信息安全技术 存储介质数据恢复服务要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39335 信息安全技术 个人信息安全影响评估指南

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

MH/T 3039—2025 民航领域数据分类分级要求

3 术语和定义

GB/T 17901、GB/T 20988—2007、GB/T 31500—2024、GB/T 35273—2020、GB/T 39335、GB/T 41391—2022、GB/T 41479—2022、MH/T 3039—2025界定的以及下列术语和定义适用于本文件。

3.1

民用无人驾驶航空器航行服务 civil unmanned aircraft air navigation service

为满足民用无人驾驶航空器飞行需要，维护和促进民用无人驾驶航空器空中交通安全和效率，由民用无人驾驶航空器航行服务提供方通过与运行人及有关管理机构之间的数据交互而实施的间隔保持、飞行引导、信息服务、预警服务、管理咨询等活动。

3.2

民用无人驾驶航空器航行服务提供方 civil unmanned aircraft air navigation service supplier

提供民用无人驾驶航空器航行服务的机构。

3.3

民用无人驾驶航空器航行服务系统 civil unmanned aircraft air navigation service system

民用无人驾驶航空器航行服务提供方提供服务时使用的数字化、信息化软硬件平台。

3.4

第三方数据提供者 third party data provider

接受民用无人驾驶航空器航行服务提供方委托，提供提升民用无人驾驶航空器航行服务能力所需数据的机构。

3.5

第三方数据 third party data

第三方数据提供者提供给民用无人驾驶航空器航行服务系统使用的数据。

4 缩略语

下列缩略语适用于本文件。

TLS：传输层安全（Transport Layer Security）

5 概述

5.1 业务组成

USS系统数据处理活动主要围绕提供民用无人驾驶航空器航行服务（以下简称“航行服务”）的业务功能开展，包括：信息类服务、管控类服务、协同类服务。

USS系统业务功能涉及的相关方包括：民用无人驾驶航空器航行服务提供方（以下简称“服务提供方”）、民用无人驾驶航空器运行人、监管方、第三方数据提供者以及其他参与USS系统数据处理活动的组织。USS系统业务功能相关方交互示意图见图 1。USS系统数据处理活动及安全风险见附录A。

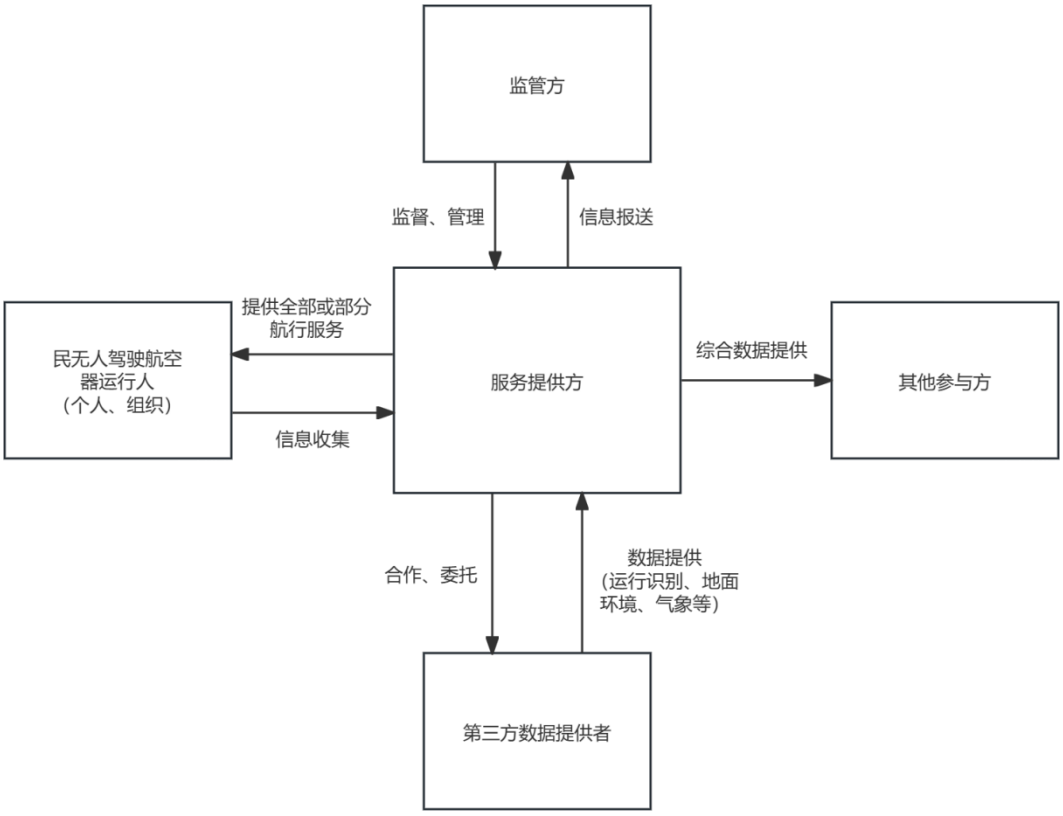


图1 USS 业务功能相关方交互示意图

5.2 数据范围

本文件中USS系统数据范围包括：

a) 用户数据：USS 系统在提供服务过程中收集和产生的运行人个人信息、组织信息，如姓名、身份证号、手机号、地址、邮箱、营业执照、通信数据等；

b) 业务数据：USS 系统在提供服务过程中处理的各类与民用无人驾驶航空器运行相关的业务数据。

6 一般要求

USS系统数据安全的一般要求如下：

a) 应识别提供航行服务过程中涉及的个人信息、敏感个人信息，并进行标识和分类管理。

b) 应在开展对个人权益有重大影响的个人信息处理活动前，按照 GB/T 39335 进行个人信息保护影响评估。

注：对个人权益有重大影响的个人信息处理活动，包括但不限于处理敏感个人信息、利用个人信息进行自动化决策、

委托处理个人信息、向其他个人信息处理者提供个人信息，公开个人信息等。

c） 应结合数据处理活动的实际情况，按照有关国家标准定期开展数据安全风险评估。

d） 应按照 MH/T 3039—2025 中 5.2 的数据分类方法和 6.3 数据分级划分的要求进行数据分类分级，识别数据处理活动中的核心数据、重要数据、一般数据，对不同级别的数据采取不同的保护措施。

注：附录 B给出了民用无人驾驶航空器航行服务系统数据分类参考示例。

e） 数据处理活动应满足 GB/T 41479—2022 中规定的要求。

f） 个人信息处理活动应满足 GB/T 35273 中规定的要求。

g） 应符合信息系统安全等级保护第二级的规定，满足 GB/T 22239 的相关要求。

7 数据收集

7.1 收集个人信息

USS系统收集个人信息应在满足GB/T 35273—2020中5.1、5.2、5.3的要求基础上，满足以下要求：

a） 通过 App 收集必要个人信息应符合 GB/T 41391—2022 中 A.8 规定；

b） 不应在运行人尚未使用任何依赖位置信息的航行服务功能前申请位置权限；

c） 收集运行人上传的文件数据时，应严格控制文件的格式和大小。

7.2 告知同意

USS系统收集运行人个人信息的告知同意应在满足GB/T 35273—2020中5.4、5.5、5.6的要求基础上，满足以下要求：

a） 在收集个人信息前明示服务提供方的名称、联系方式，个人信息的处理目的、处理方式，收集的个人信息种类、保存期限，运行人可行使权利的方式和程序，并取得同意；

b） 对用户进行实名认证时，明示依据的法律法规具体规定，并且所收集的个人信息应仅用于完成实名认证目的。

7.3 范围最小化

USS系统收集数据的范围应满足以下要求：

a） 仅收集为提供航行服务所必需的信息；

b） 收集个人信息与实现业务功能有直接关联，获取个人信息的数量是实现业务功能的最小数量；

c） 自动采集数据的频率是实现业务功能所必需的最低频率。

7.4 权限最小化

USS系统收集数据时申请的操作系统权限应满足以下要求：

a） 事先设计并公开声明收集数据所需的操作系统权限；

b） 获取的权限在实现业务功能所需的最低合理范围内。

8 数据传输

8.1 保密性

USS系统传输数据应在满足GB/T 41479—2022中5.6的要求基础上，满足以下要求：

a） 传输个人信息应满足 GB/T 35273—2020 中 6.3 的要求；

b） 传输非公开坐标数据前应加密或使用降低精度、加偏、网格化等模糊处理技术；

c） 使用数据传输安全性协议，建立加密的通信通道，例如 TLS 协议。

8.2 可用性

USS系统传输数据，宜采取以下措施：

a） 设计多条物理链路作为备份；

b） 根据数据传输需求，设计传输窗口大小、重传机制等；

c） 建立容错机制，包括错误检测和纠正；

d) 采用负载均衡技术分散数据流量；
e) 实施实时链路监测。

8.3 数据交换

USS系统与其他信息系统数据交换，应采取下列措施：
a) 在与其他信息系统建立连接之前进行双向身份认证和鉴权；
b) 通过系统接口与其他信息系统交换数据前，明确接口访问频率，设计防重复请求机制；
c) 通过系统接口与其他信息系统交换数据时，使用数据完整性保护技术；
d) 具备数据交换状态与过程监控的功能。

9 数据存储

9.1 存储和时效

USS系统存储数据，应满足以下要求：
a) 对个人信息的存储满足 GB/T 35273—2020 中 6.2、6.3、6.4 的要求；
b) 存储重要数据，采用加密、安全存储、访问控制、安全审计等措施；
c) 密钥管理根据 GB/T 17901 密钥生成、存储、分配、使用、更换、销毁等全生命周期的管理要求进行管理；
d) 个人信息存储期限应为实现个人信息处理目的所必需的最短时间，对超出保存期限应对个人信息进行删除或匿名化处理，法律法规另有规定的除外；
e) 运行监控类业务数据至少保存 12 个月，其他类别业务数据至少保存 15 个月。

9.2 备份与恢复

USS系统数据的备份与恢复，应满足以下要求：
a) 至少具有本地备份功能，根据系统的实际需求进行异地备份；
b) 数据库文件、重要日志至少每周进行一次完全备份，每天进行一次增量备份；
c) 按照 GB/T 31500—2024 中 6.4 规定的服务流程、技术手段、安全管理、服务质量的要求进行数据恢复；
d) 按照 GB/T 20988—2007 中 6.3 规定的要求配置灾难恢复资源以及 7.5 规定的实现方式完成数据灾难恢复操作。

10 数据使用

10.1 访问控制

USS系统对数据的访问控制，应满足以下要求：
a) 对个人信息的访问控制，满足 GB/T 35273—2020 中 7.1 要求；
b) 对于查询个人信息的操作，至少使用不同于用户登录的验证方式进行二次校验；
c) 通过建立审批流、限制数据访问范围等措施，限制业务数据批量查询、导出的操作；
d) 至少具有安全管理人员、数据操作人员、审计人员的角色，且根据人员的角色分配其最小所需数据访问权限。

10.2 数据展示

USS系统展示数据，应满足以下要求：
a) 事先开展个人信息安全影响评估，并依评估结果采取有效的保护措施；
b) 展示个人信息时，满足 GB/T 35273—2020 中 7.2 要求；
c) 对个人信息展示进行去标识化处理。因业务需要，确需查看未经去标识化处理的数据时，在展示界面中采用数字水印技术；
d) 在不影响正常提供航行服务情况下，展示空域、航路航线、起降场地、无人机位置的坐标数据时，采用降低精度、加偏、网格化等模糊处理方式。

10.3 数据导出

USS系统数据导出，应满足以下要求：

a) 确保业务场景设置数据导出功能的必要性；
b) 具有数据导出操作权限管控功能；
c) 具有对批量数据导出的操作进行记录和监控的功能。

10.4 第三方数据使用

USS 系统应对接入使用的第三方数据加强安全管理，包括：

a) 明确第三方数据的使用方式和范围，界定的双方数据安全保护范围和责任；
b) 宜具有对接入的第三方数据可用性、可靠性进行技术检测的能力；
c) 通过系统接口接入第三方数据，应具备对接入权限进行实时启停的控制能力。

11 数据公开与提供

USS系统公开和提供数据，应满足以下要求：

a) 对个人信息的公开应满足 GB/T 35273-2020 中 9.2、9.3、9.4 的要求；
b) 事先明确提供数据的范围，且提供数据的范围是实现业务功能的最小范围；
c) 向监管方、其他相关方提供运行人个人信息时，应告知运行人数据接收方的名称或者姓名、联系方式，个人信息的处理目的、处理方式，个人信息种类、保存期限，运行人行使权利的方式和程序，并取得同意；
d) 向运行人直接提供第三方数据时，应告知数据来源。

12 数据删除

USS系统删除数据，应满足以下要求：

a) 个人信息删除满足 GB/T 35273—2020 中 8.3 的要求；
b) 保存数据删除的有关记录，记录内容包括但不限于删除的数据类型、方式、范围、时间、责任人等。

13 日志与审计

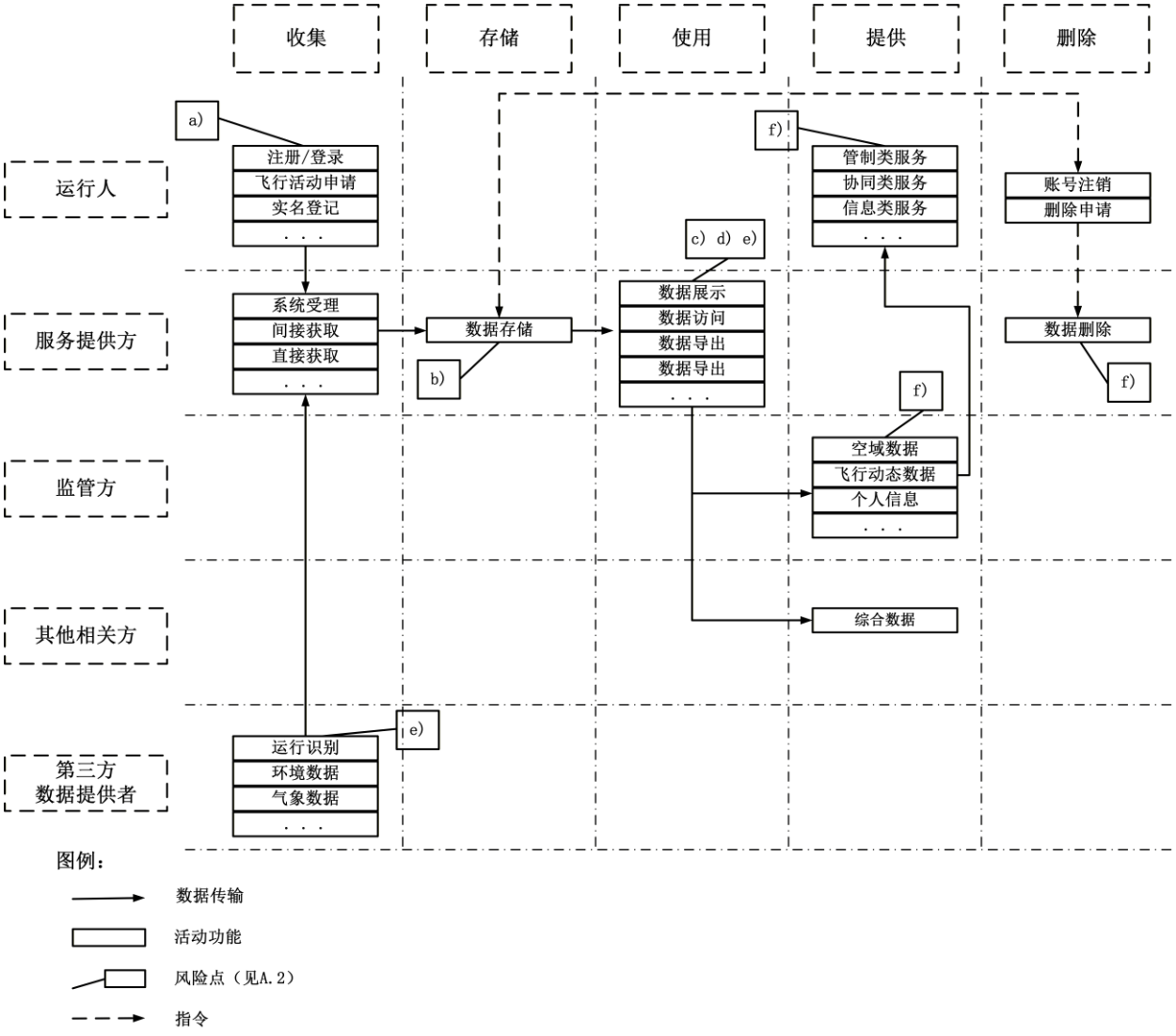
USS系统的日志与审计，应满足以下要求。

a) 对日志数据中的个人信息进行去标识化处理。
b) 记录的日志包括但不限于以下类型：
   1) 系统日志：记录系统运行状态、系统错误、系统安全等信息；
   2) 登录日志：包括用户成功登录或失败登录、正常退出、超时退出的活动；
   3) 操作日志：对用户系统操作的记录，包括访问 IP、操作类型、操作时间等；
   4) 接口访问日志：包括协议信息、目的地址和源地址、会话持续时间等。
c) 所有类别的日志记录满足以下要求：
   1) 完整性：完整记录事件的相关信息；
   2) 准确性：日志记录的时间戳、事件类型、用户标识等信息准确无误；
   3) 一致性：不同应用模块的日志格式保持一致，便于日志分析和审计；
   4) 不可篡改性：日志记录一旦生成，保证其内容不被修改。
d) 明确日志数据的存储期限，满足数据安全和隐私保护的要求。

附 录 A
（资料性）
数据处理活动及安全风险

A.1 数据处理活动

USS系统数据处理活动示意如图A.1所示。



图A.1 USS 系统数据处理活动示意图

A.2 数据安全风险

USS系统数据处理活动主要面临以下数据安全风险：

a) 在提供服务时，过度收集运行人个人信息，或过度索取操作系统权限的风险；
b) 未对个人信息与重要数据的存储采取安全防护措施，导致数据泄露的风险；
c) 未设置数据使用权限，限制数据访问范围，导致数据大规模泄露的风险；
d) 对第三方数据使用的安全管理不严格，缺少可用性、可靠性验证的技术手段，影响提供的航行服务水平；
e) 数据传输过程中未采取安全防护措施，造成系统被恶意攻击、数据被窃取的风险；

f） 未记录数据删除的时间、范围等信息，在误删数据后无法追溯、复原。

附 录 B
（资料性）
民用无人驾驶航空器航行服务系统数据分类示例参考

B.1 数据分类示例

表B.1给出了民用无人驾驶航空器航行服务系统数据一级、二级类型和典型数据分类示例。

表B.1 民用无人驾驶航空器航行服务系统数据分类示例参考

一级类别	二级类别	数据示例
空中交通管理域	空域规划	空域、航路航线、起降场地等数据
	流量管理	空域容量、空域状态、流量预测、流量控制、起降场地运行情况等数据
	运行监控	飞行动态、管制指令、电子围栏等数据
	通信导航监视	通导监信号覆盖范围、自动化航迹等数据
	气象服务	地面天气报告、空中风探测报告、气象卫星云图、气象雷达信息、雷电探测信息、天气预报、温度、气压、湿度、降水、低空风场等数据
航空服务域	通用航空（含无人机）服务	航空器实时状态、飞行计划及执行动态等数据
生产运行域	航空器	航空器实名登记标志、唯一产品识别码、性能参数等数据
	人员资质	操控员和其他民航从业人员等资质数据
宏观调控域	生产统计	运行统计与分析等数据

参 考 文 献

[1] GB/T 38152 无人驾驶航空器系统术语

[2] GB/T 42013 信息安全技术 快递物流服务数据安全要求