ICS 65.060
CCS B90

T/XJNJH

团　　体　　标　　准

T/XJNJH 011—2025

植保无人驾驶航空器数据安全管理规范

Standard for data security management of plant protection unmanned aerial vehicles

2025－12－20 发布　　2026－01－09 实施

新疆维吾尔自治区农机行业协会　　发 布

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。

本文件由新疆维吾尔自治区计量测试研究院提出。

本文件由新疆维吾尔自治区农机行业协会归口。

本文件起草单位：新疆维吾尔自治区计量测试研究院、新疆工程学院航空产业学院、新疆维吾尔自治区植物保护检疫站、新疆极目机器人科技有限公司、北京飞马航遥科技有限公司。

本文件主要起草人：武文晶、夏振奇、卓华、张玉新、肖玉琴、王立杰、高颖、赵亿坤、薛文艳、吴蓓、阿米娜·卡德尔、王鹏、王惠卿、翟辉、姜莹、郭东升。

本文件为首次发布。

植保无人驾驶航空器数据安全管理规范

1 范围

本文件规定了植保无人驾驶航空器数据安全管理的术语和定义、基本原则、设备管理要求、数据全生命周期安全要求、数据使用与禁止性规定、管理要求、监管与评估要求。

本文件适用于植保无人驾驶航空器数据采集、传输、存储、处理、共享、销毁等全流程数据活动的安全管理与合规实施的人员。

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 42590 民用无人驾驶航空器系统安全要求

GB 46761 民用无人驾驶航空器实名登记和激活要求

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 25069 信息安全技术　术语

GB/T 43071 植保无人飞机

GA/T 1143 信息安全技术数据销毁软件产品安全技术要求

MH/T 3030 民用无人驾驶航空器实名登记数据交换接口规范

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

植保无人驾驶航空器 plant protection unmanned aerial vehicle

配备液态农药、肥料等喷洒系统，通过手动、半自动或自动控制，在农林区域执行植保作业的无人驾驶航空器。

3.2

植保无人驾驶航空器数据 plant protection unmanned aerial vehicle data

植保无人驾驶航空器在运行过程中采集、产生、传输、存储和处理的各类数据，包括但不限于飞行数据、传感器数据、影像数据、位置信息以及涉及个人或组织的相关数据等。

3.3

数据安全 data security

通过采取必要措施，保障数据在其生命周期内的保密性、完整性、可用性，防止数据泄露、篡改、丢失、破坏、非法使用等，满足法律、法规及相关标准的要求。

3.4

数据采集设备 data acquisition equipment

与植保无人驾驶航空器配套，用于采集飞行参数、环境信息、影像数据、位置信息等的硬件设备，包括传感器、摄像头、定位模块、数据记录器等。

4 基本原则

4.1 合法合规原则

所有数据处理活动应符合《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规及相关标准要求。

4.2 授权同意原则

采集、使用涉及个人或组织的数据，必须获得数据所有者明确授权，无授权不得开展相关数据处理活动。

4.3 最小必要原则

仅采集、存储、使用满足业务需求的必要数据，不得过度采集无关数据或敏感信息。

4.4 安全可控原则

数据全生命周期应采取必要的技术和管理措施，确保数据安全，防范各类安全风险。

4.5 禁止牟利原则

不得利用植保无人驾驶航空器采集的数据进行非法牟利，严禁未经授权向第三方出售、转让数据。

5 设备管理要求

5.1 植保无人驾驶航空器管理

5.1.1 设备准入

使用的植保无人驾驶航空器应符合GB 42590、GB/T 43071等国家标准，具备唯一设备标识（机身序列号、设备编码），经法定检测机构检测合格并取得相关资质后方可投入使用。

5.1.2 台账管理

建立植保无人驾驶航空器设备台账，记录设备型号、序列号、采购日期、校准记录、维修记录、报废日期等信息，台账保存期限不少于设备使用年限+2年。

5.1.3 安全维护

定期对植保无人驾驶航空器进行安全检测和维护，包括飞行控制系统、通信模块、存储模块等关键部件，及时更新设备固件和安全补丁，防止设备被篡改或植入恶意程序。

5.1.4 报废管理

植保无人驾驶航空器达到使用年限或报废条件的，应先对设备内存储的数据进行彻底销毁（符合GA/T 1143要求），再进行设备报废处置，确保数据不残留。

5.2 数据采集设备管理

5.2.1 设备选型

采集设备应具备安全防护功能，支持加密存储、访问控制等安全特性，其技术参数应满足数据采集精度（符合GB/T 43071要求）和安全要求（符合GB 42590要求）。

5.2.2 身份认证

采集设备应设置独立的访问密码或生物识别认证机制，禁止使用默认密码，密码应定期更换（周期不超过90天）。

5.2.3 安全检测

定期对采集设备进行病毒查杀、安全扫描，检查设备是否存在篡改痕迹，发现异常立即停止使用并进行排查修复。

5.2.4 数据同步

采集设备与地面控制站、存储服务器之间的数据同步，应采用加密传输协议，同步过程中进行数据完整性校验，同步失败时数据应在本地加密缓存，恢复连接后优先同步。

6 数据全生命周期安全要求

6.1 数据采集安全

6.1.1 采集授权

采集涉及个人或组织的数据前，应通过书面、电子协议等形式获得明确授权，明确告知数据采集目的、范围、使用方式和保存期限；对于高敏感数据（如个人生物信息、精准地块权属信息），应单独获得专项授权。

6.1.2 采集限制

仅采集实现植保作业所必需的数据，不得采集与作业无关的个人隐私信息或组织敏感信息；采集过程中应实时校验数据合法性，自动过滤无关敏感数据。

6.1.3 采集记录

记录数据采集的时间、地点、设备编号、采集人员等信息，形成采集日志，日志保存期限不少于1年（符合GB 46761要求）。

6.2 数据传输安全

6.2.1 加密传输

采用SM4等国家认可的加密（符合MH/T 3030要求），对数据传输过程进行加密，确保数据在植保无人驾驶航空器与地面控制站、控制站与存储服务器之间传输的保密性和完整性。

6.2.2 传输协议

选用SSL/TLS等安全传输协议，建立专用安全传输通道，禁止使用明文传输协议。

6.2.3 身份认证

通信双方应进行身份认证，采用数字证书、设备唯一标识等技术手段，验证通信实体合法性，防止数据被劫持或伪造。

6.3 数据存储安全

6.3.1 存储加密

数据存储应采用加密存储方式，包括本地存储介质加密和云端存储加密，加密密钥由专人保管，定期更换（周期不超过180天）。

6.3.2 存储介质

选用加密硬盘、安全存储卡等具备安全防护功能的存储介质，对存储介质进行访问权限控制，仅授权人员可访问。

6.3.3 备份恢复

建立数据备份机制，重要数据应采用“本地+异地”双备份模式，备份周期不超过7天，保留30-90天滚动备份；制定数据恢复计划，定期开展恢复演练，确保数据丢失后可在4小时内恢复。

6.4 数据处理安全

6.4.1 访问控制

建立基于角色的访问控制机制，按“最小权限”原则分配访问权限，明确不同角色的数据访问范围；采用多因素认证（如密码+动态令牌）方式，强化身份验证。

6.4.2 数据脱敏

对涉及个人隐私或组织敏感信息的数据进行脱敏处理，采用匿名化、去标识化等技术，去除可识别主体的信息，脱敏后的数据不得反向复原。

6.4.3 处理日志

记录数据处理的操作人、操作时间、操作内容、处理结果等信息，日志保存期限不少于1年（符合GB 46761要求），确保操作可追溯。

6.5 数据共享安全

6.5.1 共享授权

数据共享前必须获得数据所有者的书面同意，明确共享范围、用途和期限；涉及高敏感数据共享的，应进行安全风险评估，经行业主管部门批准后方可共享。

6.5.2 共享防护

共享数据应先进行脱敏处理，采用加密共享、专用接口共享等安全方式，禁止通过公共网络、未加密存储介质传输共享数据。

6.5.3 第三方管理

与第三方共享数据的，应签订数据安全协议，明确第三方的数据安全责任和义务，定期对第三方的数据安全防护能力进行评估，发现问题及时终止共享。

6.6 数据销毁安全

6.6.1 销毁申请

数据达到保存期限或无需继续保存的，由数据管理部门提出销毁申请，说明销毁数据的名称、范围、原因和方式，经安全管理部门审核、上级主管领导批准后执行。

6.6.2 销毁方式

根据数据存储介质类型，采用物理销毁（如粉碎存储介质）、逻辑销毁（如符合国家标准的消磁、覆写）等方式，确保数据无法恢复；销毁过程应形成记录，包括销毁时间、地点、方式、监销人等信息，记录保存期限不少于3年。

7 数据使用与禁止性规定

7.1 数据使用规范

7.1.1 用途限制

数据仅可用于植保作业效果评估、设备运维、农业生产指导等经授权的合法用途，不得超出授权范围使用

7.1.2 禁止牟利

严禁利用采集的数据进行非法商业推广、数据交易等牟利活动，不得将数据作为商品出售、出租给第三方。

7.1.3 数据备案

运营者应在开展数据处理活动后15个工作日内，向行业主管部门备案以下信息：

（1）数据分类分级清单及敏感数据目录；

（2）数据存储位置、保存期限、备份方案；

（3）数据使用规则、共享第三方名单（如有）；
（4）数据安全管理制度及技术防护措施说明。
备案信息发生变更的，应在7个工作日内完成更新备案。

7.2 禁止性条款

禁止性条款包括但不限于以下情形：
（1）禁止未经数据所有者同意，向任何第三方出售、转让、共享数据；
（2）禁止伪造、篡改数据采集授权文件或采集日志；
（3）禁止未经安全检测的设备接入数据处理系统；
（4）禁止采用非加密方式传输、存储敏感数据；
（5）禁止销毁数据前未履行审批程序或未留存销毁记录；
（6）禁止利用数据从事危害国家安全、损害他人合法权益的活动。

8 管理要求

8.1 组织管理

8.1.1 管理机构

运营者应设立数据安全管理部门或指定专门岗位，配备专职管理人员，明确其职责的权限，负责制定和实施数据安全管理制度、技术措施，监督数据处理活动的合规性。

8.1.2 人员管理

对涉及数据处理的人员进行背景审查，签订保密协议；定期开展数据安全培训（每年不少于2次），提升人员安全意识和应急处置能力；对离岗人员及时收回数据访问权限，办理保密交接手续。

8.2 制度管理

8.2.1 管理制度

建立健全数据安全管理制度体系，包括数据分类分级管理、设备管理、采集授权管理、访问控制管理、应急处置管理等制度，明确各环节的责任主体和操作流程。

8.2.2 隐私政策

制定清晰易懂的隐私政策，明确数据处理的各项规则，在植保无人驾驶航空器使用界面、运营平台显著位置公示；隐私政策发生变更的，应提前30天告知数据所有者。

8.3 应急管理

8.3.1 应急预案

制定数据安全突发事件应急预案，明确数据泄露、篡改、丢失等事件的应急响应流程、责任分工和处置措施，应急预案应每年至少修订1次。

8.3.2 应急演练

每年至少组织1次应急演练，检验应急预案的可行性和应急处置能力，演练结束后形成评估报告，针对问题及时整改。

8.3.3 事件处置

发生数据安全事件时，应立即启动应急预案，采取封锁漏洞、停止数据传输、溯源排查等措施，防止事件扩大；在事件发生后24小时内报告行业主管部门，配合调查处理，并及时告知受影响的数据所有者。

9 监管与评估

9.1 监督机制

9.1.1 行业监督

行业主管部门应建立常态化监督检查机制，每年开展不少于1次专项检查，重点核查设备合规性、数据备案情况、安全制度落实情况、禁止性条款执行情况等；对高风险运营者（如涉及大面积作业、敏感区域作业）实施每半年1次的重点检查。

9.1.2 社会监督

建立公众举报渠道，鼓励公众、媒体对数据安全违法违规行为进行举报；对举报线索及时受理、调查，举报属实的可给予适当奖励，并对举报人信息保密。

9.1.3 技术监管

搭建数据安全动态监测平台，对接运营者数据处理系统，实时监控数据采集、传输、共享等行为，对批量数据导出、异地异常访问、敏感数据流转等风险行为自动预警，及时核查处置。

9.2 评估机制

9.2.1 自我评估

运营者应每年度开展数据安全自我评估，形成评估报告并报送行业主管部门，发现问题及时整改。

9.2.2 第三方评估

鼓励运营者委托具备资质的第三方机构开展数据安全评估，每2年至少1次；第三方机构应客观公正出具评估报告，明确风险隐患和改进建议。

参 考 文 献

[1] 中华人民共和国数据安全法
[2] 中华人民共和国个人信息保护法
[3] 中华人民共和国国务院令、中华人民共和国中央军事委员会令第761号《无人驾驶航空器飞行管理暂行条例》
[4] GB/T 32907-2016 信息安全技术 SM4分组密码算法
[5] GB/T 35273-2020 信息安全技术 个人信息安全规范
[6] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[7] GB/T 39204-2022 信息安全技术关键信息基础设施安全保护要求
[8] GB/T 39786-2021 信息安全技术信息系统密码应用基本要求
[9] MH/T 4053-2022 民用无人驾驶航空器空中交通管理信息服务系统数据接口规范