ICS 35.020
CCS L 07

MH

中华人民共和国民用航空行业标准

MH/T XXXX—XXXX

民用航空数据安全监测预警技术要求

Technical requirements for monitoring and warning of data security in civil aviation

(点击此处添加与国际标准一致性程度的标识)

（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。

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

本文件由中国民用航空局人事科教司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民用航空局信息中心、北京天融信网络安全技术有限公司、北京安华金和科技有限公司、中国民用航空局空中交通管理局、中国国际航空公司、中国民航信息网络股份有限公司等。

本文件主要起草人：张威。

民用航空数据安全监测预警技术要求

1 范围

本文件确立了民用航空（以下简称“民航”）数据安全监测预警的基本原则，规定了数据安全监测要求和预警要求。

本文件适用于指导民航领域数据处理者开展通过网络处理和产生的各种电子数据（以下简称“数据”）的安全监测和预警能力建设工作。

本文件不适用于涉及国家秘密的数据安全监测预警工作。

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 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35274 信息安全技术 大数据服务安全能力要求

MH/T XXXX 民航领域数据分类分级要求

3 术语和定义

GB/T 25069、GB/T 35273、GB/T 35274、MH/T XXXX界定的以及下列术语和定义适用于本文件。

3.1

数据安全监测 data security monitoring

通过对数据处理活动进行实时和持续的监测、分析，以便及早发现数据安全风险和事件的活动。

3.2

数据安全事件 data security incident

通过技术或其他手段对数据实施篡改、破坏、泄露或者非法获取、非法利用等导致业务损失或造成社会危害的事件。

3.3

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

[来源：GB/T 43697-2024，3.6]

3.4

告警 alert

当发现数据安全风险时，通过一定的技术手段主动发出警示类通知的行为。

[来源：GB/T 28451-2023，3.5，有修改]

3.5

预警 warning

针对即将发生或正在发生的数据安全事件，提前或及时发出安全警示的行为。

[来源：GB/T 32924-2016，3.4，有修改]

4 基本原则

民航领域数据处理者在开展数据安全监测预警时应遵循以下基本原则：

a） 安全合规：遵守国家和行业的数据安全相关管理要求，确保数据安全监测预警工作的合规性；

b） 及时准确：及时收集和分析数据安全风险信息，准确研判数据安全事件级别；

c) 全面覆盖：监测范围覆盖数据收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动；
d) 持续优化：根据实际业务场景及数据安全监测预警需求的变化，动态更新数据安全监测预警策略；
e) 最小影响：充分考虑监测活动对业务连续性的影响，避免对正常业务造成不必要的干扰或中断。

5 概述

民航领域数据处理者通过对数据处理活动进行安全监测，及时发现数据篡改、破坏、泄露或者非法获取、非法利用等数据安全风险，并对数据安全事件进行预警，从而降低数据安全事件造成的影响。

数据处理活动是数据安全监测的对象，包括数据收集、存储、使用和加工、传输、提供、公开以及删除等阶段，各阶段的内容如下：

a) 数据收集：根据特定的目的和要求，通过网络从一种或多种数据源采集数据；
b) 数据存储：将数据持久化保存在硬盘等存储介质中；
c) 数据使用和加工：对数据进行检索、展示、变换、计算、分析等操作；
d) 数据传输：通过网络将数据从一个责任主体传送到其他责任主体；
e) 数据提供：向组织内其他责任主体或其他组织提供所控制数据；
f) 数据公开：向社会公众公开所控制数据；
g) 数据删除：在所涉及的信息系统及数据存储设备中抹去数据或者覆盖存储的数据，使其不可被检索、访问。

注：由于针对存储媒体的物理销毁不能通过网络进行监测，因此本文件的数据删除不包括存储媒体物理销毁。

开展数据安全监测需要收集的信息包括但不限于支撑数据处理活动的网络设备、服务器、安全设备、密码设备、存储设备、应用系统、数据接口、数据库、大数据平台、云平台等资产的日志和流量数据，民航典型业务场景下的数据安全监测示例见附录A。

数据安全预警针对数据安全监测所发现的异常告警信息进行分析和研判，对即将发生或正在发生的数据安全事件划分预警级别，同时进行预警发布、预警响应，并根据响应情况及时升降级或解除预警。

6 数据安全监测要求

6.1 通用要求

数据安全监测应满足以下要求：

a) 对数据处理环境的网络流量进行监测，发现具有恶意代码、钓鱼邮件等特征的异常流量时进行告警；
b) 对数据接口的通信对象及行为、通信数据、接口配置进行监测，发现数据接口异常调用、异常开放、数据接口异常暴露数据、数据接口认证和鉴权机制缺陷等情况时进行告警；
c) 对数据加密、数据脱敏、数据防泄露、数据库审计等数据安全组件的日志进行监测，发现其策略未有效执行时进行告警。

6.2 数据收集

数据收集阶段应满足以下监测要求：

a) 对数据收集工具或服务组件的工作状态进行监测，发现服务异常、流量过载等异常情况时进行告警；
b) 对采用自动化工具收集核心数据、重要数据和敏感个人信息的时间、数量、频率、范围等信息进行监测，发现超业务所需范围收集数据等异常情况时进行告警；
c) 对核心数据、重要数据和敏感个人信息的数据源可靠性进行监测，发现未经鉴别或身份鉴别失败等异常情况时进行告警；
d) 对核心数据、重要数据和敏感个人信息的真实性和完整性校验结果进行监测，发现校验结果异常时进行告警。

6.3 数据存储

数据存储阶段应满足以下监测要求：

a) 对数据本地备份和异地备份的执行结果和频率进行监测，发现备份作业执行失败、备份频率过低等异常时进行告警；
b) 对访问数据存储系统的行为进行监测，发现异常 IP 访问、未授权访问等异常时进行告警；
c) 对数据存储系统的性能指标、使用空间、健康状态进行监测，发现系统过载、存储空间不足、磁盘损坏等异常时进行告警；
d) 对核心数据、重要数据和敏感个人信息的存储加密状态进行监测，发现明文存储时进行告警；
e) 对移动存储媒体接入进行监测，发现违规接入、携带恶意代码等异常时进行告警。

6.4 数据使用和加工

数据使用和加工阶段应满足以下监测要求：

a) 对数据的访问行为进行监测，发现越权访问、高频访问、异地 IP 访问、非工作时间访问等异常时进行告警；
b) 对数据的操作行为进行监测，发现批量下载、违规导出、恶意删除等异常时进行告警。

6.5 数据传输

数据传输阶段应满足以下监测要求：

a) 对数据传输设备和链路的可用性进行监测，发现设备或链路故障时进行告警；
b) 对数据传输主体的身份鉴别结果信息进行监测，发现非授权的连接时进行告警；
c) 对重要数据、核心数据和敏感个人信息的对外传输行为进行监测，发现明文传输、批量传输、超授权范围传输、未使用安全传输协议等异常时进行告警；
d) 对重要数据、核心数据和敏感个人信息的数据传输完整性校验结果进行监测，发现校验结果异常时进行告警。

6.6 数据提供

数据提供阶段应满足6.5c）的要求，还应满足以下监测要求：

a) 对核心数据、重要数据和敏感个人信息的交换、共享和转让活动进行监测，发现数据未采取加密、脱敏等措施时进行告警；
b) 对核心数据、重要数据和敏感个人信息跨境流动进行监测，发现实际出境数据与申报内容不一致等违规出境行为时进行告警。

6.7 数据公开

数据公开阶段应满足以下监测要求：

a) 对公开发布的数据进行监测，发现含有个人信息等不应公开的数据时进行告警；
b) 对公开数据的完整性进行监测，发现数据被篡改时进行告警。

6.8 数据删除

数据删除阶段应对核心数据、重要数据和敏感个人信息的删除方式、删除数据类型、删除数据量级、操作行为结果等进行监测，发现数据误删除、未经授权的数据删除等删除不当或超期留存等行为时进行告警。

7 数据安全预警要求

7.1 预警分级

数据安全事件预警级别根据数据级别和数据量级从高到低分为四个级别：红色预警（Ⅰ级）、橙色预警（Ⅱ级）、黄色预警（Ⅲ级）和蓝色预警（Ⅳ级）。

不同级别应满足以下预警要求：

a) 红色预警（Ⅰ级）：当即将发生或正在发生涉及核心数据的数据安全事件时，发布红色预警；

b) 橙色预警(Ⅱ级)：当即将发生或正在发生涉及重要数据或对社会秩序、公共利益造成轻微危害、对组织权益造成严重危害的一般数据、50 条及以上敏感个人信息的数据安全事件时，发布橙色预警；
c) 黄色预警(Ⅲ级)：当即将发生或正在发生对组织权益造成一般危害的一般数据，涉及 50 条以下的敏感个人信息的数据安全事件时，发布黄色预警；
d) 蓝色预警(Ⅳ级预警)：当即将发生或正在发生除以上提及情形外的数据安全事件时，发布蓝色预警。

7.2 预警发布

民航领域数据处理者开展预警发布工作应满足以下要求：
a) 针对监测到的数据安全异常情况进行分析和研判，将发现的数据安全风险或事件按照预警级别发布内部预警信息；
b) 确保预警发布渠道的安全可靠，避免预警信息外泄或扩散导致的数据安全事件；
c) 预警信息包含预警级别及其事件性质、涉及的数据数量、类型、影响范围和影响程度、防范对策等；
d) 当即将发生或正在发生达到黄色预警、橙色预警和红色预警级别的数据安全事件时，及时向行业数据安全监管部门报送。

7.3 预警响应

7.3.1 红色预警响应

针对红色预警，民航领域数据处理者应按以下要求开展响应工作：
a) 启动相应的应急预案，组织开展预警响应工作，联系专家和有关机构，对事态发展情况进行跟踪研判，协调组织资源调度和部门联动的各项准备工作。
b) 协调组织资源调度和部门联动的各项准备工作；
c) 实行 24 小时值班，相关人员保持通信联络畅通，数据安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查开展应急工作所需的物资，确保处于良好状态；
d) 加强数据安全事件监测和事态发展信息搜集工作，组织应急支撑队伍开展应急处置或准备、风险评估和控制工作，重要情况及时向行业数据安全监管部门汇报。

7.3.2 橙色预警响应

针对橙色预警，民航领域数据处理者应按以下要求开展响应工作：
a) 启动相应的应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作；
b) 数据安全应急技术支撑队伍保持联络畅通，检查开展应急工作所需的物资，确保处于良好状态；
c) 及时将事件处置结果或事态发展情况上报行业数据安全监管部门；
d) 对可能损害个人合法权益的数据安全事件，应当及时告知对方，并采取补救措施。

7.3.3 黄色预警响应

针对黄色预警，民航领域数据处理者应按以下要求开展响应工作：
a) 启动相应的应急预案，组织开展预警响应工作；
b) 及时将事件处置结果或事态发展情况上报行业数据安全监管部门；
c) 对可能损害个人合法权益的数据安全事件，应当及时告知对方，并采取补救措施。

7.3.4 蓝色预警响应

针对蓝色预警，民航领域数据处理者应启动相应的应急预案，组织开展预警响应。

7.4 预警升降级或解除

民航领域数据处理者根据数据安全风险或事件的动态变化，应及时发布预警升降级或解除信息，具体要求如下：
a) 当数据安全风险或事件造成的损害范围扩大、影响程度增强时，发布预警升级信息；

b） 当数据安全风险或事件得到控制，损害范围减小、影响程度降低时，发布预警降级信息；
c） 当数据安全风险或事件得到消除或经评估发现达不到蓝色预警级别时，发布预警解除信息。

附 录 A
（资料性）
民航典型业务场景下的数据安全监测示例

民航典型业务场景下的数据安全监测示例见表A.1。

表 A.1 民航典型业务场景下的数据安全监测示例

场景	产生和处理的数据	涉及的数据处理者	涉及的数据处理活动	潜在数据安全风险	对应的监测要求
旅客订票	旅客航班信息、会员信息、支付信息等	航空公司 中航信 机场 机票销售代理	收集、存储、使用和加工、传输、提供、删除	1.数据泄露风险 2.数据篡改风险 3.数据滥用风险 4.违法违规出售数据	6.1、6.2、6.3、6.4、6.5、6.6、6.8
旅客安检	旅客航班信息、旅客证件信息、旅客肖像照片、旅客安检信息、旅客状态信息、旅客登机状态、旅客行踪信息等	机场 中航信	收集、存储、使用和加工、传输、提供、删除	数据泄露风险	6.1、6.2、6.3、6.4、6.5、6.6、6.8
行李托运	行李托运信息	机场 中航信 航空公司	收集、存储、使用和加工、传输、提供、删除	1.数据泄露风险 2.数据篡改风险 3.数据滥用风险 4.数据伪造风险	6.1、6.2、6.3、6.4、6.5、6.6、6.8
旅客值机	旅客信息、航班信息、座位分配信息、行李信息等	航空公司或机场管理机构	收集、存储、使用和加工、传输、提供、删除	数据泄露风险	6.1、6.2、6.3、6.4、6.5、6.6、6.8
空中交通管理	通信导航监视、气象服务、航空情报、流量管理、运行监控等数据	地方空管局 空管分局（站）	收集、存储、使用和加工、传输、提供、删除	1.数据破坏风险 2.数据泄露风险 3.数据篡改风险 4.数据丢失风险	6.1、6.2、6.3、6.4、6.5、6.6、6.8
安全监管	行政许可信息、行政检查信息、从业人员体检信息、航空器备案信息、维修机构信息、航班信息、货邮信息、无人驾驶航空器实名登记信息等安全监管数据	民航各级行政机关	收集、存储、使用和加工、传输、提供、公开、删除	1.数据泄露风险 2.数据篡改风险 3.数据伪造风险	6.1、6.2、6.3、6.4、6.5、6.6、6.7、6.8

参 考 文 献

[1] GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南
[2] GB/T 28451-2023 信息安全技术 网络入侵防御产品技术规范
[3] GB/T 32924-2016 信息安全技术 网络安全预警指南
[4] GB/T 41479-2022 信息安全技术 网络数据处理安全要求