ICS 03.220.50
CCS V07

团 体 标 准

T/CCTAS XX—XXXX

民航旅客服务系统安全事件应急处理指南

Guidelines to emergency response of passenger service system security incidents

征求意见稿

2024.10

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国交通运输协会 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。

本文件由中国交通运输协会信息专业委员会提出。

本文件由中国交通运输协会标准化技术委员会归口。

本文件起草单位：中国民航信息网络股份有限公司、中国国际航空股份有限公司、海南航空控股股份有限公司、中国东方航空股份有限公司、厦门航空有限公司、上海吉祥航空有限公司、四川航空股份有限公司、深圳航空有限责任公司、中国民航科学技术研究院、北京时代新威信息技术有限公司。

本文件主要起草人：李征、莫鼎丞、李佳宇、王宇、毕铮、黄彩虹、杨京煜、李恩哲、张庆莉、宗深、王明、郭哲恺、温澍训、丛晓琳、吴晓明、刘刊、王优、曾福恋、王欣、许羽、朱军、宋学渊、濮小祥、李喜峰、李艳、钟山、马也、余扬、王连强。

民航旅客服务系统安全事件应急处理指南

1 范围

本指南提出了民航旅客服务系统的组织机构与职责、安全事件分类分级、安全事件应急处理准备与培训演练、安全事件应急处理流程的建议。

本指南适用于航空公司、机场及其系统运营商应急处理民航旅客服务系统安全事件。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 20985.2 信息安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 20986 信息安全技术 网络安全事件分类分级指南

GB/T 28827.3 信息服务技术 运行维护 第3部分：应急响应规范

GB/T 38645 信息安全技术 网络安全事件应急演练指南

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

MH/T 0069 民用航空网络信息安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

民航旅客服务系统 passenger service system

以面向旅客服务为核心的民航业务信息系统。

注：包括航班管理系统、订票销售系统、乘客信息管理系统、登机系统、值机系统、行李处理系统、客户关系管理系统等。

4 应急处理机制

4.1 系统用户和运维单位宜成立系统安全事件应急处理领导小组和工作组。

4.2 应急处理领导小组负责系统安全事件的应急管理工作。

4.3 应急处理工作组宜建立值班制度，具体负责本单位安全事件的应急处置工作。

4.4 宜建立职责范围和操作权限明确的应急队伍。应急队伍宜具有可靠的通信渠道，包括值班电话、短信群组、加密通讯软件等。宜定期对应急队伍成员进行专业培训，组织实战演练，模拟真实场景，检验应急预案的可行性和人员的熟练程度。

5 分类与分级

5.1 分类

参照 GB/T 20986，宜将民航旅客服务系统安全事件分为“运营故障安全事件”、“信息安全事件”和“数据安全事件”。

5.2 分级

参照GB/T 20986，宜将民航旅客服务系统安全事件级别划分为“特别重大安全事件”、“重大安全事件”、“较大安全事件”、“一般安全事件”和“轻微安全事件”。

5.3 分类分级构成

民航旅客服务系统安全事件分类分级构成见表1。

表1 民航旅客服务系统安全事件分类分级构成

	运营故障安全事件	信息安全事件	数据安全事件
特别重大安全事件	1. 系统异常导致07：00－20：00机场客运繁忙时段，全部机场离港业务不能开展60分钟以上。 2. 系统异常导致全部订座或者分销业务不能开展120分钟以上。	1. 受到持续、大量、有组织的网络攻击，导致特别严重的业务损失。 2. 系统多次病毒发作或严重发作，导致特别严重的业务损失。 3. 关键功能出现严重有害信息，对系统功能造成损害，造成特别重大社会危害。	系统中大量旅客敏感信息或业务数据泄漏，导致特别严重的业务损失或造成特别重大的社会危害。
重大安全事件	1. 系统异常导致07：00－20：00机场客运繁忙时段全部机场离港业务不能开展20分钟以上。 2. 系统异常导致年旅客吞吐量大于5000万的单个机场离港业务不能开展30分钟以上。 3. 系统异常导致全部订座或者分销业务不能开展30分钟以上。	1. 系统频繁受到多次网络攻击，导致严重的业务损失。 2. 系统多次病毒发作或严重发作，导致严重的业务损失。 3. 系统出现严重有害信息，传播广泛，造成重大社会危害。	系统中大量或者少量旅客敏感信息或相关业务数据泄漏，导致严重的业务损失，造成重大的社会危害。
较大安全事件	1. 系统异常导致07：00－20：00机场客运繁忙时段，全部机场离港业务不能开展10分钟以上的情况。 2. 系统异常导致年旅客吞吐量大于5000万单个机场离港业务不能开展20分钟以上。 3. 系统异常导致年旅客吞吐量大于2000万单个机场离港业务不能开展30分钟以上。 4. 系统异常导致全部订座或者分销业务不能开展15分钟以上。	1. 系统遭受多次网络攻击，导致较大业务损失。 2. 系统大面积病毒发作，导致较大业务损失。 3. 系统出现较严重的有害信息等，经有限传播造成较大的社会危害。	重要信息系统中少量旅客敏感信息或业务数据泄漏，导致较大的业务损失，造成较大的社会危害。

表1 民航旅客服务系统安全事件分类分级构成（续）

	运营故障安全事件	信息安全事件	数据安全事件
较大安全事件	5. 系统异常导致07：00－20：00机场客运繁忙时段，全部机场离港业务不能开展10分钟以上的情况。 6. 系统异常导致年旅客吞吐量大于5000万单个机场离港业务不能开展20分钟以上。 7. 系统异常导致年旅客吞吐量大于2000万单个机场离港业务不能开展30分钟以上。 8. 系统异常导致全部订座或者分销业务不能开展15分钟以上。	4．系统遭受多次网络攻击，导致较大业务损失。 5．系统大面积病毒发作，导致较大业务损失。 6．系统出现较严重的有害信息等，经有限传播造成较大的社会危害。	重要信息系统中少量旅客敏感信息或业务数据泄漏，导致较大的业务损失，造成较大的社会危害。
一般安全事件	1. 系统异常导致07：00－20：00机场客运繁忙时段，全部机场离港业务不能开展5分钟以上的情况。 2. 系统异常导致年旅客吞吐量大于5000万的单个机场离港业务不能开展10分钟以上。 3. 系统异常导致年旅客吞吐量大于2000万单个机场离港业务不能开展20分钟以上。 4. 系统异常导致全部订座或者分销业务不能开展10分钟以上。 5. 系统异常导致部分重要业务不能正常开展30分钟以上的情况。	1．系统受到一次网络攻击事件，导致较小的业务损失。 2．系统小范围病毒发作，导致较小的业务损失。 3．系统出现有害信息，及时发现并删除，导致较小的业务损失。	经确认的少量旅客敏感信息或业务数据泄漏，及时发现并控制，导致较小的业务损失。
轻微安全事件	1. 系统异常导致年旅客吞吐量大于5000万的单个机场离港业务不能开展5分钟以上。 2. 系统异常导致年旅客吞吐量大于2000万的单个机场离港业务不能正常开展10分钟以上。	1．系统受到一次尝试失败的网络攻击、没有导致业务损失。 2．系统无影响的病毒发作，没有导致业务损失。 3. 系统出现轻微有害信息等，及时发现并删除，没有导致业务损失。	可能的少量旅客敏感信息或业务数据泄漏，没有导致业务损失。

	3. 系统异常导致部分重要业务不能开展15分钟以上的情况。		

6 应急预案与应急演练

6.1 航空公司、机场及其系统运营商宜制定安全事件的应急预案并定期开展应急演练。应急预案宜包括预案启动条件和判断标准、事件升级流程、技术或者业务处置过程等内容。

6.2 航空公司、机场及其系统运营商宜对全体员工进行民航旅客服务系统安全意识培训，对技术和业务人员宜开展包括案例学习、应急处理流程等安全技能培训，对特别重要岗位宜获得企业或行业安全资质认证。

6.3 航空公司、机场及其系统运营商建立安全事件知识库，对民航旅客服务系统安全事件的处理知识进行管理和共享。

7 应急处理流程

7.1 监控

7.1.1 系统用户监测

系统用户在日常工作中宜关注不正常的系统提示、错误信息或性能下降等，发现服务中断、数据丢失、安全警告等异常现象后，宜尽可能保留与问题相关的截图、日志信息或其他证据，并通过客服热线、在线反馈系统向系统运营单位报告。

7.1.2 系统运营单位监测

系统运营单位宜构建包括性能监控、安全监控、日志管理的监控工具，实时捕获并响应各类应急事件，自动触发报警，告知运维人员。

7.2 报告

系统运营单位接到报警后，确认事件对客户服务造成的影响，按照应急预案设定的流程向应急处理工作组或领导小组报告，内容宜包括受影响的用户、故障发生时间等基本情况。应急处理工作组或领导小组接到报告后应立即启动应急处理流程并密切关注事件进展。

7.3 应急处理

7.3.1 应急处理方式

应急处理方式参考表2。

表2 应急处理方式

	事件	分类	分级	处理方式
1	航司系统异常	系统故障	一般事件	调查和修复

			较大事件	切换或降级
			重大事件及以上	灾备或手工
2	民航旅客服务系统异常	系统故障	一般事件	调查和修复
			较大事件	切换或降级
			重大事件及以上	灾备或手工
3	航空公司旅客数据泄露	数据泄露	一般事件	调查和修复
			较大事件	24 小时修复
			重大事件及以上	一键关停

表 2 应急处理方式（续）

	事件	分类	分级	处理方式
4	航司订票网站页面篡改	数据篡改	一般事件	调查和修复
			较大事件	24 小时修复
			重大事件及以上	一键关停
5	机票价格异常	数据错误	一般事件	调查和修复
			较大事件	功能降级
			重大事件及以上	熔断机制
6	旅客证件假冒	数据错误	一般事件	调查和修复
			较大事件	旅客行程暂停或中止
			重大事件及以上	熔断机制
7	大量旅客退票	极端操作	一般事件	调查和通报
			较大事件	联合保障
			重大事件及以上	专项小组
8	突发事件航班数据保护	极端操作	一般事件	紧急处置
			较大事件	联合保障
			重大事件及以上	熔断机制
9	机场网络故障	系统故障	一般事件	切换至冗余设备办理
			较大事件	区域切换或引导至基于公网途径办理
			重大事件及以上	切换灾备或手工模式
10	值机登机系统故障	系统故障	一般事件	调查和修复
			较大事件	切换或降级
			重大事件及以上	灾备或手工

11	配载系统故障	系统故障	一般事件	调查和修复
			较大事件	手工配载
			重大事件及以上	手工配载
12	配载系统无数据	系统故障	一般事件	调查和修复
			较大事件	手工录入数据
			重大事件及以上	手工录入数据

表 2 应急处理方式（续）

	事件	分类	分级	处理方式
13	安检数据错误	数据错误	一般事件	调查和修复
			较大事件	人工安检
			重大事件及以上	人工安检
14	航显广播篡改	数据篡改	一般事件	调查和修复
			较大事件	一键关停
			重大事件及以上	一键关停
15	机场旅客数据泄露	数据泄露	一般事件	调查和修复
			较大事件	24 小时修复
			重大事件及以上	历史数据清除
16	接口服务错误或者中断	系统故障	一般事件	调查和修复
			较大事件	切换或降级
			重大事件及以上	备用方案
17	接口流量异常	系统故障	一般事件	调查和修复
			较大事件	限流或降级
			重大事件及以上	备用方案

7.3.2 常用应急处理方式说明

7.3.2.1 系统发生安全事件后，当正常的处理手段无法快速恢复系统功能，导致短时间服务中断、功能降级、效率降低、性能下降等情况，存在整个系统业务中断的风险时，宜启用备份系统，将业务转移到备份系统。

7.3.2.2 在多机环境中部署的系统，如果系统业务模块耦合度较低，当部分服务器硬件、网络、软件等出现问题时，宜使用降级处置方式，包括暂停部分功能、断开部分用户、流量限制或者隔离服务器等。

7.3.2.3 对故障原因明确、操作方法确定的日常安全事件，宜即时修复，包括重启服务、修改系统参数、修复或删除数据等。

7.4 数据补录

当系统恢复正常后，宜进行数据检查和补录，并协助用户对应急事件的影响进行排查和补救。

7.5 分析总结

安全事件处理完毕后，宜对整个事件处理进行总结，分析识别事件发生的原因，提出改进建议，形成应急事件案例，放入安全事件知识库。

民航旅客服务系统安全事件应急处理指南
（征求意见稿）
编制说明

标准起草组

2024 年 12 月

目录

1 工作简况

1.1 任务来源

根据中国交通运输协会发布的《中国交通运输协会团体标准管理办法》之规定，本标准于2024年1月通过立项审查。

标准性质：团体标准；

归口单位：中国交通运输协会；

起草单位：中国民航信息网络股份有限公司、中国国际航空股份有限公司、海南航空控股股份有限公司、中国东方航空股份有限公司、厦门航空有限公司、上海吉祥航空有限公司、四川航空股份有限公司、深圳航空有限责任公司、中国民航科学技术研究院、北京时代新威信息技术有限公司。

1.2 目的和意义

民航旅客服务系统是民航业重要的信息系统，是维系民航业旅客业务以及运营秩序的重要信息化基础设施。根据《MH/T0069-2018 民用航空网络安全等级保护定级指南》，民航旅客服务系统属于商务/旅客服务类信息系统，支撑了中国民航业的核心业务和重要业务。其核心业务直接影响旅客流程，包括航班控制、离港控制等；重要业务涉及航空公司等民航企业的核心商业秘密和旅客个人信息，包括库存管理、订票销售等多个模块。

民航旅客服务系统作为民航业关键信息基础设施，已经完成了行业内的申报，并向国务院公安部门等备案。即民航旅客服务系统的稳定安全运营，对民航业的高效正常运转至关重要、对数以亿计的旅客信息保护至关重要，同时也是推动民航业数字化发展的核心因素。

然而，目前针对民航旅客服务系统的安全事件应急处理存在职责分工不明确、安全事件分类分级不统一、应急管理不完善等问题，不符合《中华人民共和国网络安全法》对网络安全事件应急处理要求，也与《“十四五”民用航空发展规划》《新时代民航强国建设行动纲要》等相关文件要求存在较大差距。

因此，对民航旅客服务系统中各类安全事件应急处理工作进行规范，是十分迫切且必要的。既有利于识别在民航旅客服务系统的使用和运营过程中的安全事件场景，又提升安全事件发生后的应急响应和处理能力，保障民航旅客服务系统的安全、稳定、可靠运行，降低安全事件的不良影响。同时显著降低安全事件的应急处理成本，避免负面社会影响和经济损失。

本指南的制定和实施可以明确系统安全事件分类分级标准，加强系统对于安全事件的应急响应和防护能力，在出现运营故障安全事件、信息安全事件以及数据安全事件时控制影响，最大限度减少对于民航旅客、包括航空公司、民航机场、代理机构等民航企业单位和海关边检等政府相关方的影响，保障民航旅客的合法权益和民航企业单位以及相关方等的声誉。

1.3 工作过程

为保证本标准的适用性、有效性、实用性，标准在制定过程中广泛收集了相关文献资料，包括国外相关标准与研究报告、国内相关国家标准、行业标准、地方标准等，同时开展了实地调研，为标准的研究、起草奠定了基础。具体工作过程如下：

2024 年 1 月，进行立项评审，确定由中国民航信息网络股份有限公司承担本标准的主编起草工作。根据立项评审意见，修改立项材料，完成立项。

2024 年 9 月，开展标准研究大纲评审工作。审查组专家一致同意编制大纲通过审查，并建议按照专家意见改完善后尽快开展下一阶段工作。

2024 年 9 月至 2024 年 10 月，通过典型案例的调研、问卷调查、专题研讨等形式，全面了解我国民航业各单位安全事件分类分级及应急处理流程现状，发挥标准起草单位作为市场领先的航空运输旅游业信息技术和商务服务提供商的技术业务优势，结合系统内部设计和外部特性，充分考虑到各种可能的情况，提出针对性的安全事件应急处理措施，形成标准征求意见稿草案。

2024年11月，开展标准征求意见稿草案评审工作。

2 标准制定原则与主要内容

2.1 制定原则

标准的制定本着符合国家有关法律、法规及相关政策，遵循以下原则：

（1）科学性原则：

确保指南的内容基于充分的科学证据，能够准确、客观、全面地指导民航旅客服务系统安全事件的分类分级标准、应急处理流程、应急处理准备与培训演练等内容。

（2）实用性原则：

考虑实际应用的可行性，确保指南可以被实际操作人员理解和执行。提供清晰的操作步骤和示例，便于应用。

（3）共识原则：

由多名专家参与制定，确保不同领域的知识和经验都被纳入考虑。通过共识会议、专家评审等方式达成一致意见。确保指南的适应性。

2.2 制定依据

在制定标准过程中，本标准起草组严格遵循以下标准化法律、法规、规范的规定。主要包括

1.法律法规：中华人民共和国网络安全法

2.行业标准：

MH/T 0069-2018 民用航空网络信息安全等级保护定级指南

3.国家标准：

GB/T 20985.2-2020 信息安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 28827.3-2012 信息服务技术 运行维护 第3部分：应急响应规范

GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

2.3 标准主要内容

2.3.1 范围

明确本标准的研究范围。本指南提出了民航旅客服务系统的组织机构与职责、安全事件分类分级、安全事件应急处理准备与培训演练、安全事件应急处理流程的建议。并对标准适用对象进行约束。

2.3.2 规范性引用文件

明确本标准的相关及所依赖规范性引用文件。主要包括：

GB/T 20985.2 信息安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 20986 信息安全技术 网络安全事件分类分级指南

GB/T 28827.3 信息服务技术 运行维护 第3部分：应急响应规

范

GB/T 38645 信息安全技术 网络安全事件应急演练指南

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

MH/T 0069 民用航空网络信息安全等级保护定级指南

2.3.3 术语和定义

本部分根据标准要求，设定了一个术语和定义：民航旅客服务系统。

2.3.4 应急处理机制

明确系统用户和系统运营单位针对安全事件应急处理需设置的组织机构及相应的工作职责。

2.3.5 分类与分级

参照《信息安全技术 网络安全事件分类分级指南》（GB/T 20986-2023）及民航业的行业特色，对民航旅客服务系统安全事件进行分类分级：按照“运营故障安全事件”、“信息安全事件”和“数据安全事件”进行分类；按照“特别重大安全事件”、“重大安全事件”、“较大安全事件”、“一般安全事件”和“轻微安全事件”进行分级，并提供民航旅客服务系统安全事件分类分级构成。

2.3.6 应急预案与应急演练

根据现有民航旅客服务系统各单位的安全事件应急处理经验，同时参考《网络安全事件应急演练指南》，制定安全事件应急处理的必要准备工作，包括制定专项应急预案并定期开展应急演练、开展安全培训、建立安全事件知识库。

2.3.7 应急处理流程

根据现有民航旅客服务系统应急处置实践经验，识别收集现有民航旅客服务系统的处理流程，并结合各单位特点制定统一的、体系化的安全事件应急处理流程。安全事件的主要处理过程包括安全事件监控、安全事件报告、安全事件应急处理、数据补录、分析总结等流程，并对每个过程的工作要求进行了说明，同时对安全事件应急处理方式进行了规范和描述。

3 贯彻标准的要求和措施建议

3.1 标准使用要求

本标准实施之后，民航旅客服务系统发生安全事件时系统用户和系统运营者均可遵守本标准进行应急处理。

3.2 措施建议

民航旅客服务系统系统用户单位和系统运营单位应参照本标准执行，提升应急事件发生后的应急响应和处置能力，保障民航旅客服务系统的安全、稳定、可靠运行。

4 其他需要说明的问题

4.1 预期经济效益和社会效益分析

具备成本效益：中国民航信息集团作为民航旅客服务系统专业的建设和运营单位，具有规模效应和资源整合的优势，及时响应快速处置的应急能力；同时有成熟的运维和客户体系，借助该体系可以以较低成本完成指南的编写和推广，实现成本效益最大化。

已有落地实践：由于中国民航信息集团对民航旅客服务系统的运行和管理有着深入了解，并且在部分安全事件应急处置上已经具备成功的案例。因此编写安全事件应急处理指南已经有可行的落地实践，更有可能被航空公司、机场等单位快速采纳和实施，从而降低实施成本。

长期效益：通过编写和推广安全事件应急处理指南，可以提高整个民航旅客服务系统的应急处置水平，提升安全事件的应急处理效率，降低安全事件的影响，既节约了应急处置过程成本，同时控制事件本身造成的资产损失、赔付损失以及后续由于事件发酵产生的无形资产损失。

4.2 采用国际标准和国外先进标准的一致性程度

本标准与相应的国际标准和国外先进标准在编制目的、技术内容、文本结构等方面存在较大不同，因此本标准没有采用相应的国际标准和国外先进标准。

4.3 标准实施建议

民航旅客服务系统的系统用户单位和系统运营单位在开展安全事件应急处理相关工作中，应积极采用本标准规定的安全事件分类分级建议及处置要求，以规范民航旅客服务系统的安全事件应急处理工作。

本标准与现有行业标准、地方标准无冲突，符合当下系统应急处理工作需要，建议颁布后即实施。

4.4 与有关法律、法规和强制性国家标准的关系

本标准与我国现行有关法律、法规和强制性国家标准不矛盾。

4.5 重大分歧意见的处理经过和依据

本标准在编写过程中尚未出现重大意见分歧。

4.6 其他应予以说明的事项

无。