ICS 35.020
L 07
备案号:

MH

中华人民共和国民用航空行业标准

MH/T 0028—2008

民用航空信息系统应急管理规范

Management specification for information system emergency of civil aviation

2008-03-17 发布　　2008-07-01 实施

中国民用航空局　发布

中华人民共和国民用航空
行业标准
民用航空信息系统应急管理规范
MH/T 0028—2008
*
中国科学技术出版社出版
北京市海淀区中关村南大街16号　邮政编码:100081
电话:010－62103210　传真:010－62183872
http://www.kjpbooks.com.cn
科学普及出版社发行部发行
北京长宁印刷有限公司印刷
*
开本:880毫米×1230毫米　1/16　印张:1　字数:20千字
2008年8月第1版　2008年6月第1次印刷
印数:1—500册　定价:20.00元
统一书号:175046·1043/1983

目　　次

前　言

本标准由中国民用航空局人事科教司提出并负责解释。

本标准由中国民用航空总局航空安全技术中心归口。

本标准起草单位：中国航空结算有限责任公司（原中国航空结算中心）。

本标准主要起草人：王玮、胡玉林、李爱青、江志强、杜伟军、展延奇、陈鸿。

民用航空信息系统应急管理规范

1 范围

本标准规定了民用航空信息系统应急管理(以下简称应急管理)的要求、主要阶段与主要内容。

本标准适用于民用航空信息系统突发安全事件的预警报告、应急响应、调查处理、信息披露和恢复重建等工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全等级划分准则

MH/T 0025—2005 民用航空信息系统安全等级保护管理规范

3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

接警与报告 receive warning and report

接到信息系统安全事件告警,经必要的初步研判后,依据事先确定的流程和步骤上报。

3.2

处理与响应 deal and response

依据事先确定的职责及操作的流程、步骤、内容和要求对安全事件进行处置。

3.3

关闭与解除 closing and disarm state

结束本次应急响应进程,取消本次应急响应状态。

3.4

信息安全事件 information security incident

由于自然灾害、设备软硬件故障、人为失误或破坏等原因影响到民用航空网络与信息系统的正常运行,出现业务中断、系统瘫痪、数据破坏或信息丢失泄密或窃密等现象,从而对公共安全、政治稳定、社会经济秩序造成不良影响的事件。

3.5

应急处置预案 emergency planning

针对突发事件制订的应急管理、指挥、救援计划。

注:突发事件指自然灾害、重特大事故、环境公害及人为破坏等。

3.6

应急响应 emergency response

发生突发事件后所采取的措施。

3.7

信息系统应急管理体系 information system emergency management architecture

通过规划、组织、领导、控制等措施以实现组织或机构计算机信息系统安全目标的相互关联或相互作用的一系列支撑服务要素的集合。

3.8

业务连续性规划　business continuity planning

在非计划的业务中断情况下，使业务继续或恢复其关键功能的一系列预定义的过程。

4　应急管理

4.1　要求

4.1.1　信息系统应急管理工作应按照国家与行业相关标准，落实“谁主管谁负责、谁经营谁负责”的指导原则，以应急为主要目的，以控制风险为主要目标，充分考虑信息系统的资产价值、重要程度、安全威胁和所面临的安全风险等相关要素，密切结合现实资源开展和实施。

4.1.2　在建设应急管理机制时，应考虑以下几个主要因素：

——信息共享；

——协同行动；

——快速反应；

——指导检查。

4.2　主要阶段

应急管理包括事故预防、应急准备、应急响应三个阶段。

4.2.1　事故预防

在应急管理中预防有以下含义：

——通过安全管理和安全技术等手段，尽可能地防止事故的发生，实现本质安全；

——在假定事故必然发生的前提下，通过预先采取的预防措施，来达到降低或减缓事故的影响或后果严重程度。

4.2.2　应急准备

应急准备应包括有关部门和人员职责的落实、安全隐患的辩识和风险评估、预案的编制、应急队伍的建设、应急设备(施)物资的准备和维护、预案的演习、与外部应急力量的衔接等，其目标是保持重大事故应急救援所需的应急能力。

有效的信息安全事件应急管理应进行适当的规划和准备。为使信息安全事件的响应有效，应采取下列措施：

——制订信息安全事件管理策略并使其成为文件；

——更新所有层面的信息安全和风险管理策略；

——依据现实情况制订可靠性高、操作性强的信息安全事件应急处置流程和步骤；

——编制信息安全事件应急处置预案并使其全部成为文件；

——确定信息安全事件管理的组织结构；

——按 MH/T 0025—2005 中相应的等级要求事先准备应急设备(施)物资等应急响应资源并定期检验其完备性；

——通过简报和(或)其他机制使所有的组织成员了解信息安全事件应急处置预案的存在；

——对相关人员进行培训；

——根据事先制订的演练计划，以实战演练等形式定期全面测试和评估信息安全事件应急处置流程和步骤以及应急处置预案的可靠性、有效性。

4.2.3 应急响应

4.2.3.1 通报

在事件发生之前应为事件响应作好准备。准备阶段的主要工作包括建立合理的防御、控制措施，建立适当的策略和程序，获得必要的资源和组建响应队伍等。

4.2.3.2 启动

检测阶段应做出初步的动作和响应，根据获得的初步材料和分析结果，评估事件的发生状况和影响范围，制订进一步的响应战略，并且保留可能用于司法程序的证据。

4.2.3.3 恢复

将受影响的系统和网络设备还原到正常状态。恢复工作应避免出现误操作导致数据丢失。

4.2.3.4 消除

在事件被控制之后，通过对事件的分析，找出事件根源并彻底清除。

4.2.3.5 总结和报告

在事故处置后，应对事件的起因、后果、处置方法、程序及措施进行总结和报告。

4.3 工作内容

4.3.1 机构

应成立由各级领导组成的事件应急响应指挥机构(以下简称指挥机构)，宜下设工作办公室，日常工作应由主管部门兼管。

应成立计算机应急响应工作组(以下简称工作组)，由具备专业技能的人员组成。

4.3.2 职责

指挥机构负责审批本单位突发事件应急处置预案，并组织、协调和指挥突发事件的应急处置。

工作组应在指挥机构的领导下，制订本单位突发事件应急处置预案；在发生突发事件后，接受指挥机构的命令，按应急处置预案和流程作出应急响应。

4.3.3 风险评估

应采用信息系统风险评估理论和方法定期进行风险评估，识别信息系统安全隐患和威胁。风险评估应注重：

——风险的等级及发生的概率和后果；

——持续监控风险变化，定期评估；

——确定应急处置预案的策略。

4.3.4 事件分级管理

4.3.4.1

应在风险评估的基础上，对已发生和未发生的事件实行四级管理。

4.3.4.2

事件等级分为：

——一级事件：对关键业务造成重大影响的信息安全事件；

——二级事件：对关键业务造成较重影响的信息安全事件；

——三级事件：对关键业务造成一般影响的信息安全事件；

——四级事件：对关键业务无影响的信息安全事件。

4.3.5 应急处置流程和步骤

4.3.5.1

应急处置流程为接警与报告、响应与处理、关闭与解除。

4.3.5.2

应急处置步骤包括事件的发现、上报、研判和处理。

4.3.5.3

应不断优化应急处置流程和步骤。

4.3.6 应急处置预案

4.3.6.1

应根据风险评估的结果、信息资产的价值、业务的影响、终端用户的社会经济效益等因素，分类别、分等级、分层次制订相应的应急处置预案。

4.3.6.2

可针对不同类别的突发信息安全事件，调整执行机构、应急响应资源、应急救援队伍、启动条

件、应急响应操作、应急恢复重建以及其他内容。

4.3.7 应急通报与协调

应按民航网络与信息安全信息通报要求，及时、准确地向上级汇报和向相关单位通报事故情况，必要时应按民航重大信息安全事件应急协调预案的要求向有关单位发出救援以及参与事故调查的请求。

4.3.8 应急演练

4.3.8.1 应急演练是模拟应急处置预案执行的过程，用于检验预案的可行性和效果。应依据4.3.5和4.3.6的要求，制订应急演练的计划，并明确相应的时间、地点、人员、职责、经费、设备、场景、内容等细节。其中，应模拟全部或部分的突发安全事件场景，并按应急处置预案的相关内容，在应急设备上模拟相应应急处置预案的相应应急响应操作。

4.3.8.2 应急演练分为以下类型：

——桌面演练：按照应急处置预案及流程，对情景进行口头演练；

——功能演练：针对某项应急响应功能或其中某些应急响应行动举行的演练活动；

——全面演练：应急处置预案中全部或大部分应急响应功能，检验、评价应急组织应急运行能力的演练活动。

4.3.8.3 应根据以下因素确定演练的类型：

——进行演练的潜在风险；

——现有应急响应能力；

——演练的成本。

4.3.8.4 应制订演练计划，并在报批后发至参演部门。

4.3.8.5 应对演练过程进行跟踪，并对演练过程和结果进行记录。

4.3.8.6 应对演练的效果进行评估，从而对应急处置预案可操作性、应急程序合理性、应急资源充足性做出明确的结论，并针对演练中存在的问题提出改进建议。

4.3.8.7 经过演练和改进的应急处置预案应在报批后下发。

4.3.9 事故调查

4.3.9.1 事故调查应遵循以下原则：

——独立调查原则：事故调查应独立进行，任何部门和个人不应干扰、阻碍调查工作；

——客观调查原则：事故调查应坚持实事求是的原则，客观、公正、科学地进行，不应带有主观倾向性和片面性；

——深入调查原则：事故调查应查明事件发生的直接原因，事件发生、发展过程中的其他原因，并深入分析产生这些原因的因素，包括系统设计、集成、运行、维修、运行环境和人员培训，以及规章、制度、管理办法及实施方面的缺陷等；

——全面调查原则：安全事故调查不但应查明和研究与本次事件发生有关的各种原因和产生因素，还应查明和研究与本次事件的发生无关，但在事件中暴露出来或者在调查中发现的，在其他情况下可能对信息系统安全构成威胁的所有问题。

4.3.9.2 发生重大、特别重大安全事件后，应组建事故调查组，负责事故调查。调查组成员应包括有关专家和专业技术人员。

4.3.9.3 调查组的职责如下：

——组织技术鉴定；

——查明事故发生的原因、过程、人员伤亡及财产损失情况；

——查明事故的性质、责任单位和主要责任者；

——检查控制事故的应急措施是否得当和落实；

——提出事故处理意见及防止类似事故再次发生所应采取措施的建议；

——提出对事故责任者的处理建议；

——出具事故调查报告。

4.3.9.4 调查组应向事故发生单位、有关部门及有关人员了解事故的有关情况并索取有关资料，任何单位和个人不应拒绝、阻碍、干涉调查组的正常工作。

4.3.9.5 事故调查程序如下：

——迅速获取相关原始资料；

——对现场人员进行质询，对相关记录和信息进行分析；

——召开技术复审会；

——起草事故调查报告，内容包括事故原因、性质、责任、防范措施；

——上报调查报告。

参考文献

[1]煤炭工业出版社.《完善我国安全生产监督管理体系研究》
[2]中国劳动社会保障出版社.《单位安全生产管理规章制度精选》
[3]兵器工业出版社.《生产经营单位安全生产标准化工作指南》
[4]北京交通大学出版社.《灾难恢复的规划及实施》
[5]航空工业出版社.《单位重大事故应急管理与预案编制》
[6]企业管理出版社.《应急体系建设和应急处置预案编制》
[7]《北京电子政务应急响应体系规划》
[8]《电子银行业务管理办法》(中国银行业监督管理委员会令 2006 年第 5 号)
[9]《互联网安全事件应急处理及案例》
[10]《民航网络与信息安全信息通报暂行办法》(民航人发[2004]183 号)
[11]《民航重大信息安全事件应急协调预案》(总局厅函[2005]170 号)