

ICS 03.220.50

V 07

备案号:

MH

# 中华人民共和国民用航空行业标准

MH/T 0031—2009

---

## 民用航空运输机场信息系统安全管理规范

Specification of information system security management in  
civil aviation transportation airport

2009-11-30 发布

2010-02-01 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  
民用航空运输机场信息系统安全管理规范  
MH/T 0031—2009

\*

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:010-62173865 传真:010-62179148  
<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:1.5 字数:25千字  
2009年2月第1版 2009年2月第1次印刷  
印数:1—500册 定价:30.00元  
统一书号:175046·1092/2079

## 目 次

前言	
引言	
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 管理目标	2
5 机构和职责	2
6 信息系统定级	3
7 信息系统风险评估	3
8 实施要求	3
9 应急预案	4
10 信息安全事件、事故的调查和报告	5
11 信息安全情况日常报告	5
附录 A(规范性附录) 民用机场信息安全检查表	6
附录 B(规范性附录) 民用机场信息安全检查情况反馈表	7
附录 C(规范性附录) 民用机场信息系统档案目录	8
附录 D(规范性附录) 民用机场信息安全事件、事故报告表	9
附录 E(规范性附录) 民用机场信息安全情况月报表	10
参考文献	11

## 前 言

本标准的附录 A、附录 B、附录 C、附录 D 和附录 E 为规范性附录。

本标准由中国民航华东地区管理局提出。

本标准由中国民用航空局航空安全技术中心归口。

本标准起草单位：中国民航华东地区管理局、宁波栎社国际机场。

本标准主要起草人：党宪锋、董立宏、杜伟军、江志强、关英儒。

# 引 言

随着民用机场对信息系统依赖程度的日益增强,信息系统在民航机场中的基础性、全局性作用不断增大,信息安全工作日益重要。民用机场的信息系统,直接用于保障机场航班运营、旅客服务、安全检查等日常业务运作,并用于建立与国家或地区民用航空管理机构、驻场单位及地方政府相关部门的联系。信息系统的安全,关系到国家安全和公众利益,关系到飞行安全和空防安全,关系到机场的航班正常和服务质量。各民用机场应采取有效措施,将信息系统安全风险控制在可接受的范围内,实现信息系统的持续安全。

近几年国家颁布或签发了《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)和《信息安全等级保护管理办法》(公通字[2007]43 号)等一系列有关信息安全管理政策法规。本标准根据上述国家法规和部门规章等要求制定,作为民用机场信息系统安全管理工作的依据。

# 民用航空运输机场信息系统安全管理规范

## 1 范围

本标准规定了民用航空运输机场信息系统安全管理的目标、机构和职责、信息系统定级、信息系统风险评估、应急预案、信息安全事件和事故的调查与报告、信息系统安全情况日常报告等要求。

本标准适用于民用航空运输机场信息系统安全管理。

## 2 规范性引用文件

下列文件中的条款通过在本规范中的引用而成为本规范的条款。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规范，然而，鼓励根据本规范达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

- GB/T 20984 信息安全技术 信息安全风险评估规范  
 GB/T 22239 信息安全技术 信息系统安全等级保护基本要求  
 GB/T 22240 信息安全技术 信息系统安全等级保护定级指南  
 公通字[2007] 43 号 信息安全等级保护管理办法

## 3 术语和定义

下列术语和定义适用于本标准。

### 3.1

#### 机场信息系统 **airport information system**

机场使用的由计算机、软件及其相关设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

注:机场信息系统主要包括:计算机网络系统和通信链路;航班运营类信息系统,即以航班生产保障为核心的集成系统、指挥调度系统、资源分配系统、离港控制系统、航班信息显示系统、自动广播系统、泊位引导系统、内部调度通信系统、时钟系统、货运管理系统、行李自动分拣系统、助航灯光系统等;智能控制类信息系统,即以楼宇自动化为核心的UPS供电系统、楼宇自控系统、地理信息系统、智能消防报警系统等;安全防范类系统,即以空防安全为核心的安检信息管理系统、视频监控系統、门禁系统等;通用管理类信息系统,即以办公自动化为核心的电子政务系统、企业资源规划系统、门户网站、电子商务系统等。

### 3.2

#### 可用性 **availability**

根据授权实体的要求可访问和利用的特性。

[ISO/IEC13335-1:2004]

### 3.3

#### 完整性 **integrity**

保护资产的准确和完整的特性。

[ISO/IEC13335-1:2004]

### 3.4

#### 保密性 **confidentiality**

信息不能被未授权的个人、实体或者过程利用或知悉的特性。

[ISO/IEC13335-1:2004]

### 3.5

#### **连续性 continuity**

系统服务状态或通过系统服务实现的业务运营状态得以持续的特性。

### 3.6

#### **风险评估 risk assessment**

风险分析和风险评价的整个过程。

[ISO/IEC Guide 73:2002]

### 3.7

#### **信息安全事件 information security incident**

一个信息安全事件由单个或一系列的有害或意外信息安全事态组成,它们具有损害业务运作和威胁信息安全的极大的可能性。

[GB/T 22080—2008]

### 3.8

#### **信息安全事故 information security accident**

由各种原因导致出现业务中断、系统瘫痪、关键数据丢失或核心信息失窃等,从而在国家安全、社会稳定或公众利益等方面造成不良影响以及造成一定程度经济损失的事件。

## 4 管理目标

机场信息系统安全管理的目标是规范机场信息系统的管理,保证机场信息系统的可用性、保密性和完整性,实现机场相关业务的连续性。

## 5 机构和职责

### 5.1 管理机构

机场信息系统安全的管理,应由专门的管理机构负责。该机构应由机场主管领导担任负责人,成员应包括财务、规划、安全监察、设备、技术部门和合同管理等部门负责人,以及各信息系统的主要用户单位的负责人。

管理机构的工作职责应包括:

- a) 贯彻落实各级行政管理机构关于保障信息安全的法规、规章及国家和行业标准;
- b) 审批、发布本单位信息系统安全相关的管理办法、规章制度,批准与信息系统安全相关的重要事项;
- c) 界定和分配信息系统安全管理职责,建立信息系统安全目标责任制度和安全责任追究制度;
- d) 协调信息系统应急演练;
- e) 组织调查、处理信息安全事件和事故;
- f) 对信息系统安全建设、改造等重大事项进行决策,安排信息系统安全建设、运行保障和技术培训专项资金及人员岗位。

### 5.2 实施机构

机场信息系统安全管理机构应下设实施机构,管理机构各成员单位均应指派专人作为实施机构的成员。

实施机构工作职责应包括:

- a) 起草机场信息系统安全规划和相关规章制度;
- b) 编制信息系统安全工作的年度计划和资金预算,组织实施有关项目;
- c) 组织实施信息系统定级和风险评估;

- d) 监督和指导相关制度、规范在机场内部和各驻场单位的落实,并收集信息系统安全信息和  
建议;
- e) 负责信息安全通报、信息安全事件和事故报告,开展有关信息安全的宣传、培训、咨询等工作;
- f) 组织完成上级交办的其他信息安全相关工作。

### 5.3 信息系统安全管理岗位

机场应设置信息系统安全管理岗位,该岗位基本职责应包括:

- a) 监督信息系统安全相关规定在各部门的落实情况和相关人员的执行情况;
- b) 具体承办信息安全事件、事故的调查处置;
- c) 具体承办信息系统等级保护和信息系统风险评估工作;
- d) 起草和修订信息系统安全管理规章制度、规范。

## 6 信息系统定级

### 6.1 定级范围

机场各信息系统均应按照公通字[2007]43号、GB/T 22239和GB/T 22240的要求定级。

### 6.2 定级方式

6.2.1 机场信息系统实行自主定级。

6.2.2 系统定级应由业务部门和技术部门共同承担。

### 6.3 定级备案

6.3.1 机场信息系统定级后,应将定级相关的书面文件报地区民用航空管理机构备案。

6.3.2 定级为二级(含)以上的信息系统,应按要求向当地公安机关备案。

## 7 信息系统风险评估

7.1 应按GB/T 20984的要求对信息安全等级为二级(含)以上的信息系统进行周期性风险评估。

7.2 评估工作完成后,应将评估相关的书面文件报地区民用航空管理机构备案。

7.3 应根据评估结果和整改建议,落实信息系统安全整改和安全加固方案。

## 8 实施要求

### 8.1 安全责任

8.1.1 机场信息安全主管领导应对信息系统安全负领导责任。

8.1.2 机场信息系统运行保障单位应承担信息系统的技术安全管理责任。

8.1.3 信息系统用户单位应承担信息系统的使用安全管理责任。

8.1.4 信息系统接入单位应承担信息系统的接入安全管理责任。

8.1.5 信息系统的提供单位应承担信息系统的源数据安全安全管理责任。

### 8.2 检查和考核

8.2.1 机场应将信息安全保障情况列为年度安全责任考核的内容,各单位应将本单位的信息安全责任落实到具体岗位和人员。

8.2.2 应定期对信息安全管理制度的落实情况进行自查,检查内容应形成书面文件,日常检查的重点内容见附录A。

8.2.3 应通过国家或地区民用航空管理机构的信息安全检查,检查情况反馈表见附录B。机场应根据检查反馈意见进行整改,并将整改情况及时上报。

### 8.3 教育和培训

8.3.1 有关岗位员工应接受信息安全培训并通过相关考核。



- 8.3.2 每年应至少组织一次针对信息系统用户的信息安全培训和考核。
- 8.3.3 应组织对信息系统安全管理和技术维护人员进行安全理论和技能的专业培训和考核。
- 8.3.4 适用于系统用户的操作规程和说明,应以书面文件的形式下发到所有用户单位,此类文件的送达应有规范的文档记录。用户单位应组织学习和落实此类文件。

#### 8.4 运行和维护

- 8.4.1 各信息系统均应建立档案等规范性文件,见附录 C。
- 8.4.2 应对规范性文件的实用性、有效性、可操作性进行定期核查、修订,并应进行严格的版本控制。
- 8.4.3 各信息系统的检查、维护应指定专人负责,应明确各系统检查维护的内容、周期,并记录相关信息。
- 8.4.4 有备份措施的系统应定期验证备份措施的可用性,并建立规范的文档记录。
- 8.4.5 各信息系统运行、检查、维护的规范性文件记录应至少保存 3 年。

#### 8.5 工作区

信息系统设备机房、重要操作岗位等区域应设置连续的视频监控,监控录像应至少保存 30 d(天),应具备安防设施,防止未经授权人员进入。

#### 8.6 远程访问

- 8.6.1 信息系统远程访问的批准,以及访问时间、访问权限和内容等涉及信息系统安全的操作应可被本地管理员控制。
- 8.6.2 应严格控制远程支持和服务,如需此类服务,应与服务方签订保密协议。
- 8.6.3 应对远程访问的各类信息建立规范的文档。
- 8.6.4 访问结束后应立即断开物理链接。

#### 8.7 信息系统的隔离

- 8.7.1 承载敏感信息和重要数据的信息系统应采取有效的隔离措施,防止超范围发布或泄漏。
- 8.7.2 专用业务信息系统应与互联网隔离。

#### 8.8 安全防护系统建设

- 8.8.1 新建或升级改造的信息系统应按照等级保护要求实施安全防护系统建设。
- 8.8.2 信息安全防护系统应与新建或升级改造信息系统的建设同步规划、同步建设、同步投入运行,并确定系统的安全保护等级。
- 8.8.3 新建或升级改造的信息系统建成后,应根据安全保护等级进行验收。

### 9 应急预案

#### 9.1 制订和管理

- 9.1.1 应分别制订信息系统的技术应急预案和业务应急预案。
- 9.1.2 技术应急预案指当信息系统出现异常时,技术部门为尽快恢复系统功能而采取的一系列应急措施,此类预案应由技术部门负责起草、修订和执行。
- 9.1.3 业务应急预案指当信息系统出现异常时,系统用户为确保本岗位业务和(或)服务运作连续性而采取的一系列应急措施,此类预案应由系统用户单位负责起草、修订和执行。
- 9.1.4 各类预案应明确启动条件、组织者、指挥者、参加者及其责任和操作步骤、规范,形成正式文件并下发到相关部门。
- 9.1.5 应急预案制定或修订后,应下发到相关部门,各部门应组织对相关人员进行培训。

#### 9.2 演练

- 9.2.1 应定期组织应急演练,检查应急预案的可行性和有效性。

9.2.2 演练结束后,应进行总结和分析,并修订完善应急预案。

## 10 信息安全事件、事故的调查和报告

### 10.1 调查

10.1.1 机场信息安全管理机构组织对信息安全事件、事故进行调查。

10.1.2 不安全事件、事故发生后,应保留相关信息,以备检查和处理。

### 10.2 报告

10.2.1 信息安全事件发生后,应在 4 h 内上报事件报告表,见附录 D。

10.2.2 信息安全事故发生后应立即向国家、地区民用航空管理机构报告,并在 4 h 内上报事故报告表,见附录 D。

## 11 信息安全情况日常报告

11.1 应在规定日期前将机场信息安全日常情况和信息安全事态上报地区民用航空管理机构,报表格格式见附录 E。

11.2 敏感和重要时期的信息安全情况报告应按地区民用航空管理机构要求执行。

11.3 应向各驻场单位通报相关信息系统安全信息。

附录 A  
(规范性附录)  
民用机场信息安全检查表

表 A.1 为民用机场信息安全检查表。

表 A.1

序号	项 目	实现	未实现	备注
1	建立了信息安全管理机构,支持信息安全管理工作的			
2	设立了信息系统安全岗位,并具有相应的人员编制			
3	配备了足够数量的技术管理人员,信息系统应指定专人进行维护管理			
4	信息安全工作有年度计划和经费预算,并确保预算得到批准和落实			
5	对技术管理活动进行了制度化、规范化管理			
6	建立并不断完善、健全安全管理制度			
7	信息安全工作在系统用户部门得到落实			
8	建立恰当可靠的联络渠道,以便安全事件发生时能迅速传递相关信息并得到支持			
9	对人员的系统管理、使用行为进行控制和规范			
10	对技术人员的管理活动有书面文件作为指导			
11	对信息系统进行合理定级,落实相应的等级保护基本要求,并进行备案管理			
12	对信息系统进行周期性风险评估,并及时落实整改措施			
13	落实了信息安全责任制			
14	应确保软件开发、测试过程和工程实施过程中的安全,有专门的不停航施工保障要求			
15	确保安全工程的实施质量和安全功能的准确实现			
16	机房等重要区域具有良好、安全的运行环境			
17	对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制			
18	信息系统检查、巡视、记录等技术维护工作有周期性和连续性			
19	对支撑设施、硬件设备、存储介质、备用设备进行周期性检查和维护,确保其实时可用性			
20	所有信息系统用户具有与其岗位相适应的应用能力,应对新用户进行相关培训			
21	各类技术人员具有与其岗位相适应的技术能力,年度技术培训应有计划并落实专项资金			
22	对各类人员进行相关的安全、风险常识和意识教育			
23	向系统最终用户提供的足够的系统操作和使用手册等资料			
24	任何变更控制和设备使用均应经过申报和审批,并对其实行制度化的管理			
25	在事件发生后能采取积极、有效的应急策略和措施,应急预案应形成文件			
26	应急预案进行周期性演练、总结和修订,确保其可行性和有效性			
27	按要求及时上报信息安全相关报表、报告			

附录 B  
(规范性附录)  
民用机场信息安全检查情况反馈表

表 B.1 为民用机场信息安全检查情况反馈表。

表 B.1

单位名称				
序号	问题描述	问题归属		
合计				
机场代表 (签字)		检查组成员 (签字)		日期

附录 C  
(规范性附录)  
民用机场信息系统档案目录

民用机场信息系统档案目录包括：

- a) 系统基本信息,包括:
  - 1) 设备清单(名称、型号、出厂日期、数量、保修期、供货商、技术支持电话等);
  - 2) 操作系统(名称、版本号、补丁情况等);
  - 3) 数据库(名称、版本号、补丁情况等);
  - 4) 备份软件(名称、版本号等);
- b) 操作规程;
- c) 维护规程;
- d) 日常巡检单;
- e) 技术应急预案;
- f) 业务应急预案;
- g) 典型故障案例分析;
- h) 重大故障处置记录;
- i) 重要维护保养记录。

附录 D  
(规范性附录)  
民用机场信息安全事件、事故报告表

表 D.1 为民用机场信息安全事件、事故报告表。

表 D.1

通报单位名称				通报日期	
系统名称与功能					
事故类型、影响范围、 损失及危害情况					
初步分析研判结果和 已采取的应对措施					
部门领导 (签字)		填表人 (签字)		联系电话	

附录 E  
(规范性附录)  
民用机场信息安全情况月报表

表 E.1 为民用机场信息安全情况月报表。

表 E.1

通报单位名称		通报日期	
<p>信息系统安全状况</p> <p>日常检查和报告的内容应包括：</p> <ol style="list-style-type: none"> <li>1. 信息系统通信和资源使用异常,网络与信息系统瘫痪、应用服务中断或数据篡改、丢失等情况；</li> <li>2. 信息系统受病毒感染或网络被攻击等情况；</li> <li>3. 网站、电子邮件等网络信息服务中反动、有害信息的传播情况；</li> <li>4. 利用网络从事违法犯罪活动的情况；</li> <li>5. 其他影响网络与信息安全的状况。</li> </ol> <p>发生信息系统安全事件时,应详细报告系统名称、时间、地点、厂商名称、责任单位、责任人、事件状态、影响情况、排查处置情况等。</p>			
部门领导 (签字)		填表人 (签字)	联系电话

## 参考文献

- [1] ISO/IEC 27001 信息安全管理要求
  - [2] ISO/IEC 17799 信息安全管理实用规则
  - [3] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
  - [4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
  - [5] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
  - [6] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
  - [7] GB/T 18336—2000 信息技术 信息技术安全性评估准则
  - [8] GB/T 19716—2005 信息技术 信息安全管理实用规则
  - [9] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
  - [10] NIST Special Publication 800—53 联邦信息系统推荐性安全控制措施
  - [11] DoD Directive & Instruction 8500—1,2 信息保障 & 信息保障实施
  - [12] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
-