ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0035—2012

民用航空网络与信息安全管理规范

Specification for civil aviation network and information security management

2012-02-08 发布　　2012-06-01 实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民用航空局航空器适航审定司批准立项。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学、中国民航科学技术研究院。

本标准主要起草人：杨宏宇、杜伟军、马晓宁、谢丽霞。

民用航空网络与信息安全管理规范

1 范围

本标准规定了民用航空网络与信息安全管理目标、网络与信息安全管理职责、网络与信息系统等级保护、网络与信息安全管理、网络与信息安全应急与处置，以及网络与信息安全技术保障与服务。

本标准适用于民用航空网络与信息安全管理。

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，仅所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。

MH/T 0026 重要信息系统灾难恢复指南

MH/T 0028 民用航空重大信息安全事件应急协调预案

3 术语与定义

下列术语和定义适用于本标准。

3.1

网络与信息安全 network and information security

依靠网络进行的信息交互活动中的信息安全性，以及网络与信息系统自身的安全可靠性，特指网络和信息系统的保密性、完整性和可用性，以及信息的可认证性、可核查性、不可抵赖性和可靠性。

3.2

信息安全事件 information security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

3.3

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密等，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。

3.4

民用航空重要网络与信息系统 important network and information system of civil aviation

安全保护等级为二级以上的民用航空网络和信息系统，包括空管通信网、商务数据网，以及民用航空运输机场、航空公司、空管部门和航空运输保障单位的基础网络和核心业务系统等。

4 管理目标

通过制定民用航空网络与信息安全管理规范，建立民用航空网络与信息安全管理体系，实现民用航空业网络与信息安全管理工作的规范化、标准化，有效实施民用航空业网络与信息安全管理和民用航空各企事业单位的网络与信息安全工作，推进民用航空网络与信息安全管理水平的提升。

5 管理职责

民用航空各企事业单位应：

a) 建立本单位的网络与信息安全管理机构和网络与信息安全责任制，设置网络与信息安全专职岗位；
b) 制定和完善本单位网络与信息安全策略和规章制度，建立和健全网络与信息安全管理、等级保护、信息通报、应急演练、灾难备份、评估审计、教育培训、信息保密等制度，组织开展网络与信息安全专项培训，增强网络与信息安全意识，提高网络与信息安全防护技能；
c) 检查和监督本单位网络与信息安全工作，定期开展网络与信息安全风险评估、安全审计等专项工作；
d) 制定网络与信息安全应急处置预案，并及时处置和上报网络与信息安全事件、事故；
e) 落实上级网络与信息安全主管部门开展的其他网络与信息安全工作。

6 信息安全等级保护

6.1 民用航空网络与信息系统应实行信息安全等级保护制度。民用航空各企事业单位应按照相关文件和标准的要求，建立健全并落实符合相应等级要求的网络与信息安全责任制、人员安全管理制度、系统建设管理制度和系统运维管理制度等安全管理制度。

6.2 民用航空各企事业单位应按照相关文件和标准的要求，建立并落实信息安全等级保护监督检查机制，定期对各项信息安全等级保护管理制度的落实情况进行自查。

6.3 民用航空各企事业单位应对本单位所运营、使用的网络和信息系统进行安全保护等级定级。对于二级（含）以上网络和信息系统，应当在安全保护等级确定后 30d(天)内，到当地公安机关办理备案手续，并将备案材料报所辖地区行业行政主管部门备案。

6.4 网络和信息系统的安全保护等级确定后，民用航空各企事业单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定并满足信息系统安全保护等级需求的信息技术产品，开展网络和信息系统的安全建设或者改建工作。

6.5 在网络和信息系统建设和改建过程中，民用航空各企事业单位应按照相关文件和标准的要求，同步建设符合该等级要求的信息安全设施。

6.6 对于安全保护等级为二级（含）以上的网络和信息系统，民用航空各企事业单位应按照相关文件和标准的要求建立并落实网络和信息系统的安全测评与风险评估制度，每年开展一次系统安全测评和风险评估。在重点保障任务时期，对安全保护等级为三级（含）以上的网络和信息系统进行专项安全测评和风险评估。

6.7 民用航空各企事业单位的涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

6.8 民用航空各企事业单位应接受民用航空各级行政管理机构检查，并根据整改通知要求，按照等级保护管理规范和技术标准进行整改，将整改报告向所辖地区行业行政主管部门备案。

7 网络与信息安全管理

7.1 民用航空各企事业单位网络与信息安全管理部门应建立与业务管理部门以及生产安全管理部门的管理协调机制。

7.2 民用航空各企事业单位应加强对民用航空重要网络与信息系统的安全防护建设和安全维护，依照等级保护相关要求，按照同步规划、同步建设、同步运行的原则完善系统安全保障措施。

7.3 民用航空各企事业单位应按照相关要求，对已投入运行的网络和信息系统要制定信息安全改造规划，定期升级和更新安全保障设施并保证信息安全经费的投入。

7.4 民用航空网站服务实行备案制度，政务和商务网站的开通和运行应遵守国家关于网站管理和信息发布的各项法律、法规，并报所辖地区行业行政主管部门备案。

7.5 民用航空各企事业单位应按照国家有关保密规定和标准，建立、健全涉密信息保密制度，加强对涉密信息、互联网站和生产运行信息系统的管理和保护，采取物理隔离、不应在非涉密计算机和移动存储设备上存放秘密等级以上的文件或数据等措施，保护载有涉密内容的计算机系统和信息。

7.6 民用航空各企事业单位应建立计算机病毒和非法入侵防范管理制度，制定有效措施防止网络与信息系统受到非法攻击或计算机病毒的侵扰，安装和使用经认证的计算机病毒防治产品并定期更新。

7.7 民用航空各企事业单位应建立民用航空重要网络与信息系统的灾难备份与恢复制度，灾备系统建设和管理应符合 MH/T 0026 的要求。重要信息系统的数据中心、备份中心不应设立在境外，核心数据不应委托境外机构处理。

7.8 民用航空各企事业单位应建立风险评估与预警制度，要定期对本单位技术队伍、外部环境和信息系统安全现状、管理和技术措施等开展风险评估和安全审计，根据评估结果进行整改。

7.9 民用航空各企事业单位应落实信息安全管理自查制度，对照信息安全管理检查表逐条开展自查，信息安全管理检查表见附录 A。民用航空各企事业单位应对检查中发现的问题进行研究分析，制定整改方案和实施计划，填写年度信息安全检查情况报告表并按要求上报，年度信息安全检查情况报告表见附录 B。

8 网络与信息安全应急管理

8.1 民用航空各企事业单位应建立通报制度，落实负责通报工作的责任人，按要求向所辖地区行业行政主管部门及时上报、通报本单位网络与信息系统的安全工作情况。

8.2 民用航空各企事业单位发生重大信息安全事故时，应立即向行业行政主管部门报告。

8.3 民用航空各企事业单位发生网页篡改事件时应及时上报。

8.4 民用航空各企事业单位应建立、健全应急管理制度，结合现有资源不断完善应急预案，定期开展各种形式的预案演练等工作，并对演练情况及时总结，根据演练中暴露的问题，修改完善预案。

8.5 民用航空各企事业单位应按照 MH/T 0028 的要求，建立与当地相关行政管理部门的应急协调机制，及时处理由电力供应、网络中断和网络攻击引发的信息安全事件、事故。

9 网络与信息安全技术与服务管理

9.1 民用航空重要网络与信息系统的安全建设应由国家认可的具有信息安全资质的单位承担。系统运行管理单位在系统建成后应组织安全验收。系统的网络与信息安全服务，应由具备相应服务资质的单位和人员承担，并应与服务单位签署保密协议。

9.2 网络与信息系统建设采购的安全专用产品应通过国家的安全认证，网络与信息技术产品应符合有关技术标准的要求。采用国外网络与信息技术产品应由具有计算机信息系统集成资质的国内企业代理，未安装网络与信息安全防护设备和未经网络与信息安全评估认证的网络与信息系统不应投入运行。

9.3 与互联网连接的民用航空重要网络与信息系统应采取有效的防护措施，并与国家网络与信息安全专业机构建立安全技术服务关系，定期进行安全监测与评估。

9.4 已投入运行的民用航空重要网络与信息系统要定期进行安全测评，对达不到相关安全标准等级的网络与信息系统，应限期整改。对整改后仍达不到等级保护安全标准的网络与信息系统，不应继续使用。

9.5 民用航空各企事业单位应根据安全等级保护和相关保密规定，对各类办公、生产运营网络与信息系统采取访问控制措施，加强对远程访问的严格控制和管理，需要远程技术支持和服务的，应与提供服务方签订安全协议。

附　录　A
（规范性附录）
民航信息安全管理检查表

一、信息安全组织管理	
1.信息安全管理机构及其工作开展情况	（1）国家与行业信息安全法规标准和工作要求的执行情况； （2）组织制定信息安全工作计划或工作方案情况； （3）组织制定并落实信息安全管理规章制度情况； （4）组织开展信息安全教育培训和督促检查工作情况； （5）信息安全信息通报工作的执行组织和情况； （6）信息系统等级保护工作开展情况，包括系统定级、备案和整改测评。
2.信息安全岗位和人员及其工作开展情况	（1）各单位信息安全岗位和人员设定情况； （2）信息安全员工作职责及开展督促、检查和指导等日常工作情况。
二、日常信息安全管理	
1.人员管理。查验相关文档、文件、记录等	（1）各工作岗位信息安全和保密责任制落实，特别是重要岗位信息安全和保密协议签订情况； （2）人员离岗离职信息安全管理情况； （3）外部人员访问重要岗位和机房等重要区域管理情况； （4）违反制度规定造成信息安全事件的责任查处情况等。
2.信息资产管理。查验相关文档、台账、记录等	（1）信息资产管理制度建立及落实情况，资产台账是否清晰、账物是否相符； （2）办公软件、应用软件等安装与使用情况，是否安装了有与工作无关的软件； （3）计算机及相关设备维修维护、报废销毁管理情况，是否有相应的登记记录等。
3.信息技术外包服务安全管理	重点检查系统开发、系统集成、运行维护、灾难备份、数据处理、安全检测、系统托管等外包服务的安全管理。包括： （1）服务机构性质与背景情况，是否由外资机构提供服务； （2）服务合同及安全保密协议签订情况，安全责任是否明晰； （3）人员现场服务记录情况，是否有现场服务监管措施； （4）系统维护方式情况，重点排查远程在线服务带来的安全风险； （5）灾难备份建设和服务情况。
4.信息技术产品使用管理	（1）办公用计算机、公文处理软件、信息安全设备、服务器、网络设备等使用产品的安全可控情况； （2）本年度新采购办公用计算机、公文处理软件、信息安全设备是否满足安全可控要求。
5.信息安全经费保障	（1）信息安全防护设施建设、运行、维护、检查及管理等费用是否纳入部门年度预算； （2）本年度信息安全经费实际投入情况等。

三、信息安全防护管理	
1.网络边界防护管理	重点检查系统总体网络架构、子系统分布、终端节点、区域划分及边界防护措施等，包括： （1）网络分区分域合理性； （2）安全防护设备策略配置有效性； （3）互联网接入情况，是否有访问互联网的安全控制措施，是否留存互联网访问日志并定期进行分析。
2.信息系统安全管理	重点检查信息安全风险评估、等级保护等安全管理制度落实情况，包括： （1）服务器安全防护。重点检查服务器上应用、服务、端口以及系统补丁等情况，是否关闭了不必要的应用、服务、端口；账户口令强度和更新情况；病毒木马防护情况，是否使用技术工具定期进行漏洞扫描、病毒木马检测； （2）网络设备防护。重点检查网络设备安全策略配置的有效性；账户口令强度和更新情况；是否使用技术工具定期进行漏洞扫描； （3）信息安全设备部署及使用。重点检查防病毒、防火墙、入侵检测、安全审计等安全设备部署及使用情况，以及安全策略配置的有效性。
3.门户网站安全管理	以防攻击、防挂马、防篡改、防瘫痪、防窃密为目标，对门户网站安全防护情况进行全面检查，包括： （1）系统管理账户和口令、清理无关账户、防止出现空口令、弱口令和默认口令； （2）服务器补丁更新情况，关闭不必要的端口，停止不必要的服务和应用，删除不必要的链接和插件； （3）网站目录结构，删除临时文件，防止敏感信息泄露； （4）信息发布审核制度建立及落实情况； （5）是否使用技术工具定期进行漏洞扫描、木马检测。
4.电子邮箱安全管理	（1）邮箱使用情况，是否有非本部门人员特别是无关人员使用； （2）账户口令强度以及更新情况，是否使用技术措施控制和管理口令，口令强度是否符合要求、是否定期更新。
5.终端计算机安全管理	（1）是否采取集中安全管理措施； （2）账户口令强度和更新情况； （3）接入互联网安全措施（如实名接入认证、对计算机 IP 和 MAC 地址进行绑定等）； （4）是否使用技术工具定期进行漏洞扫描、病毒木马检测； （5）在非涉密信息系统和涉密信息系统间混用情况； （6）使用非涉密计算机处理涉密信息情况
6.移动存储设备安全管理	（1）是否采取集中安全管理措施； （2）是否配备必要的电子消磁或销毁设备； （3）在非涉密信息系统和涉密信息系统间混用情况
四、信息安全应急管理	
1.应急预案	重点检查本部门信息安全应急预案制定、修订、备案及宣贯培训情况。
2.应急演练	重点检查信息安全应急预案演练情况；已开展演练的，查看演练文档、记录（包括演练计划、演练方案、演练记录、演练总结报告等）。
3.应急技术支援。	重点检查是否明确了应急技术支援队伍；已明确的，检查其服务合同及安全保密协议签订情况，了解掌握应急技术支援队伍基本情况以及开展的技术支援活动。

4.灾难备份	重点检查重要数据和重要信息系统备份情况；对采用社会第三方灾备服务的，检查其服务合同及安全保密协议签订情况，了解掌握灾难备份服务设施运维安全管理情况。
5.信息安全事件应急处置	重点检查本年度发生的信息安全事件及处置情况；发生过重大信息安全事件的，检查是否进行了及时处置，是否对事件原因进行分析并制定改进措施，是否按照要求上报和通报。
五、信息安全教育培训	
重点检查信息安全和保密形势教育及警示教育情况，领导干部和机关工作人员参加信息安全基本技能培训情况，信息安全管理和技术人员参加信息安全专业培训情况等。	
六、各单位信息安全自查工作开展情况	
1.在检查中发现问题的整改情况	（1）制定的整改计划及采取的整改措施； （2）整改效果以及是否开展了进一步的信息安全风险评估； （3）年度检查情况报告完成情况，是否按要求及时报送，报告是否完整准确、符合要求。
2.本年度检查工作开展情况	（1）检查工作责任制建立和检查工作经费落实情况； （2）检查工作方案制定及组织实施情况； （3）采取的安全保密和风险控制措施，检查人员、有关文档和数据的安全保密管理情况。
3.安全技术检测	是否组织技术力量，使用必要的技术工具，对服务器、终端计算机、网络设备以及门户网站等信息系统进行安全检测，排查病毒木马、安全漏洞等。

附 录 B
（规范性附录）
_____年度信息安全检查情况报告表

一、部门基本情况(在相应项目的空白处填写信息)	
部门名称	
分管信息安全工作的领导 （本部门副职领导）	①姓名： ②职务：
信息安全管理机构 （如办公厅）	①名称： ②负责人：　　职务： ③联系人：　　电话：
信息安全专职工作处室 （如信息安全处）	①名称： ②负责人：　　电话：
二、信息系统基本情况(在相应项目的空白处填写数据，在符合项目的“□”上划“√”)	
信息系统情况	①信息系统总数：　　个 ②面向社会公众提供服务的信息系统数：　　个 ③委托第三方进行日常运维管理的信息系统数：　　个 ④本年度经过安全测评（含风险评估、等级测评）系统数　　个
系统定级情况	第一级：　　个　第二级：　　个　第三级：　　个 第四级：　　个　第五级：　　个　未定级：　　个
互联网接入情况	互联网接入口总数：　　个 其中：□联通　接入口数量：　个　接入带宽：　　兆 □电信　接入口数量：　个　接入带宽：　　兆 □其他：　　接入口数量：　　个 　　接入口带宽：　　兆
三、日常安全管理情况(在符合项目的“□”上划“√”)	
人员管理	①岗位信息安全责任制度：□已建立　□未建立 ②重要岗位人员信息安全和保密协议： □全部签订　□部分签订　□均未签订 ③人员离岗离职安全管理规定：□已制定　□未制定 ④外部人员访问机房等重要区域审批制度：□已建立□未建立
资产管理	①资产管理制度：□已建立　□未建立 ②设备维修维护和报废管理： □已建立管理制度，且维修维护和报废记录完整 □已建立管理制度，但维修维护和报废记录不完整 □尚未建立管理制度

四、信息安全防护管理情况(在符合项目的“□”上划“√”)	
网络边界防护管理	①网络访问控制：□有访问控制措施　□无访问控制措施 ②网络访问日志：□留存日志　　□未留存日志 ③安全防护策略设置：□使用默认设置　□根据应用自主设置
门户网站安全管理	①网页防篡改措施：□已部署　　□未部署 ②网站信息发布管理：□已建立审核制度，且审核记录完整 □已建立审核制度，但审核记录不完整 □尚未建立审核制度
电子邮箱安全管理	①邮箱使用：□仅限本部门工作人员使用 □除本部门工作人员外，还有其他人员在使用 ②账户口令管理：□使用技术措施控制和管理口令强度 □无口令强度限制措施
终端计算机安全管理	①终端计算机安全管理方式： □使用统一平台对终端计算机进行集中管理 □用户分散管理 ②接入互联网安全控制措施： □有效控制措施（如实名接入、绑定计算机 IP 和 MAC 地址等） □无控制措施
存储介质安全管理	①存储阵列、磁盘库等大容量存储介质安全防护： □外联，但采取了技术防范措施控制风险 □外联，无技术防范措施 □不外联 ②移动存储介质管理方式： □集中管理，统一登记、配发、收回、维修、报废、销毁 □未采取集中管理方式 ③电子信息消除或销毁设备：□已配备　□未配备
五、信息安全应急管理情况(在相应项目的空白处填写数据，在符合项目的“□”上划“√”)	
信息安全应急预案	□已制定　本年度修订情况：□修订　□未修订 □未制定
信息安全应急演练	□本年度已开展，共演练　　次　　□本年度未开展
信息安全灾难备份	①重要数据：□备份　□未备份 ②重要信息系统：□备份　□未备份
应急技术支援队伍	□部门所属单位　□外部专业机构　□无
六、信息技术产品应用情况(在相应项目的空白处填写数据)	
服务器	总台数：　　，其中国产台数： 使用国产 CPU 的服务器台数：
终端计算机 （含笔记本）	总台数：　　，其中国产台数： 使用国产 CPU 的计算机台数：
网络交换设备 （路由器、交换机等）	总台数：　　，其中国产台数
操作系统	①服务器操作系统情况： 安装 Windows 操作系统的服务器台数：

		安装Linux操作系统的服务器台数： 安装其他操作系统的服务器台数： ②终端计算机操作系统情况： 安装Windows操作系统的计算机台数： 安装Linux操作系统的计算机台数： 安装其他操作系统的计算机台数：
数据库		总套数：　　，其中国产套数：
公文处理软件 （终端计算机安装）		安装国产公文软件的终端计算机台数： 安装国外公文处理软件的终端计算机台数
信息安全产品		①安装国产防病毒产品的终端计算机： ②防火墙（不含终端软件防火墙）台数： 其中国产防火墙的台数：
七、信息安全教育培训情况(在相应项目的空白处填写数据)		
培训人数		本年度接受信息安全教育培训的人数：　　人 占本部门总人数的比例：　　%
培训次数		本年度开展信息安全教育培训的次数：　　次
专业培训		本年度信息安全管理和技术人员参加专业培训：　人次
八、信息安全经费预算投入情况(在相应项目的空白处填写数据)		
经费预算		本年度信息安全经费预算额：　　万元
经费投入		本年度信息安全经费投入额：　　万元 （上一年度信息安全经费投入额：　　万元）
九、本年度信息安全事件情况(在相应项目的空白处填写数据)		
本年度安全技术检测结果	病毒木马等恶意代码检测结果	①进行过病毒木马等恶意代码检测的服务器台数： 其中感染恶意代码的服务器台数： ②进行过病毒木马等恶意代码检测的终端计算机台数： 其中感染恶意代码的终端计算机台数：
	漏洞检测结果	①进行过漏洞扫描的服务器台数： 其中存在漏洞的服务器台数： 存在高风险的服务器台数： ②进行过漏洞扫描的终端计算机台数： 其中存在漏洞的终端计算机台数： 存在高风险的终端计算机台数：
本年度信息安全事件统计	门户网站受攻击情况	本部门入侵检测设备检测到的门户网站受攻击次数：
	网页被篡改情况	门户网站网页被篡改（含内嵌恶意代码）次数：
	设备违规使用情况	①使用非涉密终端计算机处理涉密信息事件数： ②终端计算机在非涉密系统和涉密系统间混用事件数： ③移动存储介质在非涉密系统和涉密系统之间交叉使用事件数：

<table>
<tr><td colspan="3">十、信息技术外包服务机构情况，包括参与技术检测的外部专业机构(在相应项目的空白处填写信息，在符合项目的“□”上划“√”)</td></tr>
<tr><td rowspan="5">外包服务机构 1</td><td>机构名称</td><td></td></tr>
<tr><td>机构性质</td><td>□国有　□民营　□外资</td></tr>
<tr><td>服务内容</td><td></td></tr>
<tr><td>信息安全保密协议</td><td>已签订　□未签订</td></tr>
<tr><td>信息安全管理体系认证情况</td><td>□已通过认证
认证机构名称：
□未通过认证</td></tr>
<tr><td rowspan="4">外包服务机构 2</td><td>机构名称</td><td></td></tr>
<tr><td>机构性质</td><td>□国有单位　□民营单位　□外资企业</td></tr>
<tr><td>服务内容</td><td></td></tr>
<tr><td>信息安全管理体系认证情况</td><td>□已通过认证
认证机构名称：
□未通过认证</td></tr>
<tr><td rowspan="5">外包服务机构 3</td><td>机构名称</td><td></td></tr>
<tr><td>机构性质</td><td>□国有单位　□民营单位　□外资企业</td></tr>
<tr><td>服务内容</td><td></td></tr>
<tr><td>信息安全和保密协议</td><td>□已签订　□未签订</td></tr>
<tr><td>信息安全管理体系认证情况</td><td>□已通过认证
认证机构名称：
□未通过认证</td></tr>
<tr><td colspan="3">（如有三个以上外包机构，每个外包机构均有填写，可另附页）</td></tr>
</table>