中国民用机场协会网络与信息安全管理办法

第一章 总则

第一条 为进一步增强中国民用机场协会（以下简称“机场协会”）网络与信息系统安全规范能力，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）和《民航网络与信息安全管理暂行办法》等有关法律法规，结合协会实际情况，特制定本办法。

第二条 本办法所指的网络信息与安全管理，是指由计算机（包括相关和配套设备）为终端设备，利用计算机、通信、网络等技术，以协会名义开展信息化管理工作中的数据采集、处理、存储和传输的设备、技术、管理的组合，包含但不限于保障计算机网络设备和配套设施的安全、信息的安全、运行环境的安全。

第三条 本办法适用于以机场协会名义建设使用的网络信息系统。按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，对网络与信息安全实施管理。

第二章 组织机构及职责

第四条 成立机场协会信息安全工作领导小组（以下简称领导小组），组长由秘书长担任，成员由副秘书长和各部门（分支机构）负责人组成，负责机场协会信息安全工作的组织领导与工作协调。机场协会网络安全管理责任人为协会分管副秘书长，机场协会网络安全运行和维护责任人为协会网络信息主管。

第五条 领导小组负责研究重大事件，落实国家和行业相关政策和研究制定信息安全总体策略等。职责主要包括：

（一）执行国家和民航信息安全的法律、规章、标准，组织开展协会信息安全工作；

（二）建立信息安全管理机构，设置信息安全管理部门安全专职岗位，落实信息安全责任制；

（三）建立健全信息安全管理体系，落实信息安全管理经费；

（四）制定信息安全应急管理预案，不定期开展业务培训；

（五）落实行业网络信息安全通报、自查制度；

（六）配合行业管理部门开展信息安全检查和安全事件调查，对发现问题进行整改；

（七）完成国家社团组织管理机构和行业管理部门交办的其他信息安全工作。

领导小组下设办公室，由秘书处综合部负责，组织协会各分支机构及秘书处各部门承担网络信息基础规划建设、组织管理、安全风险评估、相关业务考核及培训等日常具体工作。

第三章 日常管理

第六条 加强网络数据安全和保密意识。

（一）禁止下载互联网上任何未经确认其安全性的软件，安装新软件时，需要获得协会网络管理人员授权。任何单位和个人不得利用单位分配的个人电子邮箱上公网注册信息，不得访问恶意网站和不健康网站，不要随意打开陌生邮件，打开邮件后发现其为钓鱼邮件或仿冒邮件应立刻关闭退出，并向协会网络管理人员报告。禁止打开邮件系统邮件自动转发功能。

（二）网络系统的所有软件均不准私自拷贝出来赠送其它单位或个人，违者将严肃处理。

（三）严禁随意使用 U 盘、光盘等存储介质，如工作需要，外来 U 盘、光盘须在没联网的单机上检查病毒，确认无毒后方可上网使用。

（四）发现病毒，应及时对感染病毒的设备进行隔离，情况严重时报交流部并及时妥善处理。实时进行防病毒监控，做好防病毒软件和病毒库的智能升级。

（五）应当注意保护网络数据信息的安全，对于存储在数据库中的关键数据，以及关键的应用系统进行及时数据备份，及时更新数据库和防病毒软件病毒库，定期对所有数据库进行漏洞扫描、补丁修复，保证重要数据的安全。应打开操作系统自动更新功能，确保及时更新修补漏洞。

（六）机场协会应设立专（兼）职工作人员并签订保密协议；

第七条 建立信息资产管理制度，建立资产台账，每年度至少维护更新一次；

第八条 信息技术外包服务安全管理事项：

（一）委托专业技术公司提供技术支持和远程服务；

（二）签订服务合同及安全保密协议，履行相关义务，督促落实信息安全责任；

（三）记录维护人员现场服务情况；

（四）排查远程在线服务带来的安全风险；

（五）检查督导外包公司进行数据备份建设，提供技术支持和数据存储管理服务。

第九条 信息安全防护设施建设、运行、维护、检查及管理等费用纳入年度预算。

第十条 离职人员办理离职手续时，应将机场协会工作业务相关电子信息资料完整移交给明确的接收人员；未经协会同意，不得擅自拷贝复制及使用、对外泄露相关信息，否则将依法追究其法律责任。

第四章 应急管理

第十一条 结合工作实际，机场协会应制定信息安全应急预案，并不定期开展应急演练，每年度至少开展一次。

第十二条 根据实际需求与应急技术支援团队（外包服务方）签署服务合同或协议，明确相应权责关系、响应时限。

第十三条 按照《信息安全等级保护管理办法》确定的技术标准，建立机场协会信息安全技术等级保护制度，并定期检查，进行问题整改，确保运行正常。

第五章 病毒防治

第十四条 机场协会所有计算机终端设备必须安装防病毒软件，并保持防病毒软件病毒库信息的及时更新。

第十五条 网络管理人员必须了解最新的病毒信息和病毒动向，及时检查并下载杀毒防毒补丁。

第十六条 内部计算机终端用户必须启用防病毒产品的实时检测功能，任何主机系统和终端在加载任何软件或数据前，先对该软件或数据进行病毒检查。

第十七条 由于个人计算机系统漏洞或者误操作导致计算机感染病毒程序的，必须及时切断本机网络连接。在病毒发作时，必须进行相应的诊断、分析和记录，对于因计算机病毒而引起的重要信息系统瘫痪、程序和数据损坏等重大事故，及时报告本部门负责人以及综合部，及时进行处理。

第六章 监督管理

第十八条 所有部门和个人在网络上应自觉遵守网络信息安全的有关规定。在办公网络上严禁下列行为：

（一）查阅、复制或传播违反国家法律、扰乱社会秩序，封建迷信，恶意诽谤他人等不良信息。

（二）破坏、盗用计算机网络中的信息资源和危害计算机网络安全的活动。

（三）盗用他人帐号、盗用他人 IP 地址。

（四）私自转借、转让用户帐号造成危害。

（五）故意制作、传播计算机病毒等破坏性程序。

（六）不按国家和政府有关规定擅自开设二级代理接纳网络用户。

（七）上网信息审查不严，造成严重后果。

（八）以端口扫描等方式，破坏网络正常运行。

第十九条 按照行业管理部门要求，由机场协会领导小组不定期组织开展协会网络与信息系统安全检查工作，每年度至少检查一次。

第二十条 机场协会员工必须自觉遵守本制度，提高信息安全保密、防范意识，防止泄密事件的发生。对在信息安全管理工作中成绩突出的部门和个人年终给予表彰奖励；对发生信息安全事件并造成一定影响的部门和个人，按规定作出处理；涉及秘书处相关部门（分支机构）及个人的，应纳入机场协会绩效考核体系管理。

第七章 附 则

第二十一条 本管理办法由机场协会秘书处负责解释。

第二十二条 本管理办法自颁布之日起执行。

附件 1：

中国民用机场协会网络安全事件应急预案

第一章 总则

本预案的适用范围为中国民用机场协会的网站、网络安全设施设备的网络安全事件应急处理。

第一条 日常安全工作职责

中国民用机场协会工作人员根据分工、做好以下工作：

（一）对网站、网络进行日常检查、分析风险、排除隐患、做好网站数据备份，形成日常工作机制，预防安全事故发生。

（二）制定相关安全事件的预警方案和解决方案。

（三）掌握网络网站技术发展趋势，不断提升安全防范水平。

（四）及时处置各类突发安全事件。

第二条 安全应急处置原则

（一）报告原则：发生突发安全事件，第一时间向机场协会信息安全工作领导小组报告，同时积极进行处置，处置全程要及时汇报工作进展。

（二）安全原则：处置安全事件时，要科学客观，首先保证人员安全，其次保证设备数据安全。

（三）效率原则：处置突发事件要及时迅速，讲究方法，善于协调，争取在最短时间内解决问题。

（四）协调配合原则：出现大规模故障后，根据工作需要，积极配合，协同处理，提高工作质量与效率。

第三条　安全应急事件处置

（一）安全事件定义分类

一般故障：指区域性网络安全事件，具体包括：局部网络瘫痪、个别设备死机、网站服务器停止工作等。

重大故障：指发生大规模或整体性网络瘫痪、个别硬件设备损坏或被窃、数据丢失或网站遭恶意篡改破坏等。

特大故障：指机房发生火灾或遭可抗拒力破坏造成机房损毁及人员伤害等。

（二）处置时限

发生突发安全事件，一般故障 2 小时内解决，重大故障 24 小时内解决，特大故障 48 小时内解决。

（三）处置措施

发生突发事件，工作人员第一时间报告领导并进行处置。迅速准确判断事件原因,在保证人员、设备、数据安全的前提下，进行针对性处置。属一般性故障的，机场协会工作人员及时进行处置；属设备损坏的，要及时报告网络主管根据领导安排进行合理处置；属系统故障的，要及时联系维护公司进行处置；属遭受攻击的，要及时取证留存，并由维护公司进行处置。必要时，通知有关单位做好应对。事后总结本次事件处置情况，形成分析报告。

第二章 网站安全应急处置

第四条　日常维护

（一）机场协会人员每天对网站进行查看，密切监视信息内容。每天上午和下午各检查网站和 OA 系统一次，查看运行情况。

（二）检查各服务器杀毒软件及防火墙升级情况，及时给系统打补丁。

第五条　安全事件分类及应急处置办法

（一）硬件故障

指因自然灾害、供电不正常、人为因素等造成的服务器硬件损坏、丢失情况。

1、 OA 系统工作人员每季度对其进行检测,维护公司每季度进行软硬件检测，并填写记录，每年度进行汇报。

2、发生硬件损坏或丢失后要立即报告网络主管，并联系设备供应商及有关单位处理。

（二）攻击、篡改类故障

指网站系统遭到网络攻击不能正常运作，或出现非法信息、页面被篡改。

1、发现网站出现非法信息或页面被篡改，要第一时间对其进行删除，恢复相关信息及页面，同时报告网络主管，必要时可对网站服务器进行关闭，待检测无故障后再开启服务。

2、网站维护员要妥善保存有关记录及日志或审计记录，并立即追查非法信息来源，将有关情况进行上报，情况非常严重的要向公安部门报案。

（三）病毒木马类故障

指云端服务器感染病毒木马，存在安全隐患。

1、每周对服务器杀毒安全软件进行系统升级，并进行病毒木马扫描，封堵系统漏洞。

2、发现服务器感染病毒木马，要立即对其进行查杀，报告网络主管，根据具体情况，通知联网的相关单位进行终端的病毒木马查杀。

3、由于病毒木马入侵服务器造成数据丢失或系统崩溃的，要第一时间报告网络主管，并联系相关单位进行数据恢复。

（四）系统类故障

指网站系统由于长时间运行或系统存在的 bug 造成网站不能正常运行。

1、相关负责人要每月对网站数据进行备份，并进行存档。

2、发现此类问题，要报告网络主管，并联系网站维护单位进行检测修复。

第六条　应急保障

（一）记录服务器供应商及网站维护公司电话，出现问题能及时联络处理。

（二）协会人员应学习各类软硬件知识，提高应对和处理突发网络故障的能力。

第三章　网络安全应急处置

第七条　日常维护

（一）每季度对设备进行例行检查及卫生保洁，检查项目包括设备运行状态、温度、供电及设备周边环境是否安全。

（二）每年对协会分会各单位进行调查访问，查看实际情况。

第八条　应急处置

（一）发生故障后，首先排查故障范围，确定软件、硬件故障，是光路故障还是以太网故障。

（二）对于大面积网络故障或硬件线路设备损坏，要第一时间报告网络主管。

（三）如发生光路设备故障，及时联络联通公司客户经理协调处理。

（四）如发生以太网故障，要及时进行处理，必要时联系设备供应商及相关单位联合处理。

第四章 中心机房及办公区安全应急处置

第九条　用电安全

（一）坚持正确的用电规范。

（二）不使用超负荷电器设备。

（三）不随意改变工程设计的供电线路。

（四）每天下班，最后离开办公室的人员关闭办公区主电源。

（五）每两个月对中心机房各电源设备进行检查。遇节假日，除关闭办公区主电源外，检查中心机房内电源和线路，确保设备安全稳定运行。

（六）发生火警事件发生后，机房人员应根据所属区域和现场情况，判断和选择正确的方法，及时上报协会领导，同时配合相关人员处置，降低事件带来的影响。

1、对于设备发生烟雾，机房主管人员协同相关人员寻找烟雾点并切断相关区域电源。

2、当设备发生可以控制火情时，机房主管人员应协同相关人员进行灭火工作。

3、当主机房发生火灾而无法控制，应采取其他施救措施。

第十条 空调及通风设备

正常情况：

温度：冬季： 18℃-22℃±2℃ 夏季： 18℃-25℃±2℃

温度变化≤5℃/H

湿度：40%-60%±5%

每周对中心机房温湿度进行监控，防患于未然。

空调系统故障导致机房内温度、湿度升高或设备出现温度告警等异常现象时，执行以下步骤：

（一）首先查看故障空调的位置和现象，联系学院后勤加紧维修。

（二）如果故障较为严重，影响范围大，则立即汇报给网络主管。

（三）启用风扇、加湿器等设备降低室内温度、湿度，并打开机柜门和房间门，以便于设备散热和空气流通。

（四）相关工作人员要密切注意各设备的运行情况，如出现告警，查看日志了解情况，必要时请设备厂家派人立即赶到现场进行技术支持。

（五）相关负责人员对各个维护业务进行检查，如已经影响到系统和业务的正常运行，尤其是一些重要业务，应立即汇报分管领导，做进一步处理。

（六）若此时空调已修好，室内温度、湿度恢复正常或在下降中，相关负责人员对各个设备的运行情况详细检查，确保恢复正常。

（七）待室内温度、湿度恢复正常并监控一段时间后无异常，将风扇、加湿器关闭并放回原位，保持机房卫生和整洁。

（八）相关负责人员对此次故障做好记录。

第十一条　核心设备安全

（一）根据实际情况对核心设备进行检查，确保设备安全稳定运行。

（二）发生核心设备硬件故障后，工作人员应及时报告网络主管，并查找、确定故障设备及故障原因，进行先期处置。同时联系设备提供商共同检测并排除故障。

（三）若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（四）故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系厂商进行返厂维修或调换设备。

第十二条　数据安全与恢复

（一）日常使用维护参照《机场协会网络与信息安全管理办法》中第三章各项进行。

（二）发生业务数据损坏时，工作人员应及时报告网络主管，检查、备份系统当前数据。

（三）数据损坏事件较严重无法保证正常工作的，经部门领导同意，及时通知各部门以手工方式开展工作。

（四）协会应待数据系统恢复后，检查基础数据的完整性；重新备份数据，并写出故障分析报告。

第十三条　其他事项

（一）无关人员未经批准不得进入机房。

（二）对各设备和线路进行维护或改造，需经协会分管领导批准，由工作人员陪同进行。

（三）使用充分控干水份的抹布及拖把进行保洁，尽量不使用干布或扫帚，避免扬尘。

（四）保洁时，注意不要触碰电源接口及网络接口等，以免漏电或导致线路接触不良。

附件 2:

中国民用机场协会网站安全责任书

为保障网络与信息安全，维护国家安全和社会稳定，保护公民、法人和其他组织的合法权益，本人在从事机场协会网站管理运行维护过程中，郑重承诺严格履行相关法律义务，承担以下责任：

一、严格遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《民航网络与信息安全管理暂行办法》、《中国民用机场协会网络与信息安全管理办法》等法律法规和规章的有关规定，结合协会实际情况，依法从事互联网电子公告服务。对本单位网站的信息服务行为承担法律、行政、民事责任。

二、建立和完善网络安全技术措施，定期进行安全风险分析与系统漏洞测试，防止病毒传播和被非法控制为网络攻击的跳板，适时对软硬件进行升级，确保系统安全可靠运行。

三、完善信息安全管理制度和技术防范手段，建立健全公共信息内容自动过滤系统和人工值班监控制度，不采取、实行《中国民用机场协会网络与信息安全管理办法》第十八条规定的禁止性行为，自觉遵守法律规范，认真履行社会责任。

四、在管理运行维护过程中发现安全事故及时控制和处理，保留有关原始记录，并在24小时内向相关主管部门报告。

五、遵守机房安全管理制度。严格保守国家秘密，确保不泄漏用户个人资料。

六、依法接受相关管理部门的监督管理和检查，主动向通信管理部门提供软件过滤系统远程登录检查条件。

七、本责任书（承诺书）随运维协议生效之日起生效。

安全责任人：

签署日期：