新疆民航网络安全管理办法

第一章　总　则

第一条　为规范新疆民航网络安全工作，提高网络与信息系统安全防范能力，保障新疆民航网络安全，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》《新疆维吾尔自治区网络安全管理条例》《国家网络安全事件报告管理办法》《民航网络与信息安全管理暂行办法》《民航网络安全工作责任制考核办法》等法律、行政法规、有关规定制定本办法。

第二条　本办法适用于民航新疆管理局（以下简称“管理局”）及所属监管机构（以下简称“监管局”）和辖区企事业单位（以下简称“辖区单位”）的网络安全工作。

第三条　新疆民航网络安全工作按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，采取“积极防御、综合防范”的方针，坚持保障网络安全与促进信息化发展相协调、管理与技术统筹兼顾的原则，实行统一协调、分级管理、分工负责。

第四条　辖区单位对本单位的网络安全负主体责任，其主要负责人是本单位网络安全的第一责任人。管理局、监管局负监管责任。

第二章　职责与分工

第五条　管理局负责辖区内民航网络安全监督管理工作，履行下列职责：

（一）依照国家和民航网络安全法律、法规、规章和标准，制定辖区内民航网络安全工作制度，指导辖区单位开展网络安全工作；

（二）监督辖区单位网络安全规划和建设；

（三）建立网络安全年度检查制度，实施年度检查以及重点保障时期的专项检查；

（四）建立网络安全应急机制和通报体系，向民航局通报辖区网络安全信息，报送新疆民航网络安全年度总结，协助民航局开展网络安全事件调查和处理；

（五）承办民航局交办的其他网络安全工作。

第六条　各监管局承担本辖区民航网络安全监督检查工作，主要职责包括：

（一）依照国家和民航网络安全的法律、规章和标准，制定网络安全工作制度，指导本辖区民航各单位的网络安全工作；

（二）落实管理局的网络安全年度检查计划，开展本辖区民航各单位的网络安全检查工作；

（三）建立本辖区网络安全信息通报体系，向管理局通报本辖区网络安全信息，报送本辖区网络安全年度总结报告，协助民航局开展网络安全事件调查和处理；

（四）落实民航局、管理局部署的其它网络安全工作。

第七条 辖区单位网络安全工作的主要职责是:

（一）执行国家和民航行业网络安全法律、法规、规章与标准，编制网络安全规划，制定网络安全管理制度;

（二）建立网络安全管理机构，明确本单位网络安全管理部门，设置网络安全员专职岗位，落实网络安全责任制;

（三）采取技术措施和其他必要措施，保障网络安全，有效应对网络安全事件，防范违法犯罪活动;

（四）落实网络安全经费，建设和完善网络安全保障基础设施，开展网络安全等级保护、风险评估、安全自查、安全培训等工作，保护旅客信息和生产数据安全;

（五）建立网络安全信息通报制度，配合民航行政管理机构进行网络安全检查和事件调查，对发现问题进行整改;

（六）制定网络安全应急预案，定期开展应急演练;

（七）承担民航行政管理机构部署的其他网络安全工作。

第三章 网络安全一般规定

第八条 辖区单位应当建立健全人员、资产、采购、外包、系统建设与运维、备份、应急等网络安全管理制度，对网络安全各项事宜进行统一规范管理。

第九条 辖区单位应当建立信息系统（包括网络设施、云计算平台、大数据平台、物联网系统、工业控制系统等）资产管理

制度，编制资产清单，明确资产管理责任部门与人员，定期对照资产清单对资产进行一致性检查并保留检查记录。

第十条 辖区单位应当选用符合国家有关规定、安全可控的信息技术产品和服务，采购的信息安全产品和服务应由具备资格的机构安全认证合格或者安全检测符合要求。

第十一条 辖区单位应当建立网络信息技术外包服务和远程技术服务安全管理制度，需要外包服务或远程技术服务的，应当与提供者签订安全保密协议。

第十二条 辖区单位应当建立网络安全经费保障制度，将网络安全经费纳入本单位年度财务预算，按照同步规划、同步建设、同步运行的原则，建立和完善安全保障措施，新建系统中网络安全建设经费的实际投入应当不低于系统建设总经费的15%。

第十三条 辖区单位应当依照国家标准规范开展计算机机房建设，制定机房安全管理制度，对出入机房人员进行审查、登记。

第十四条 辖区单位应当严格网络信息系统接入管理，建立系统接入审批制度。在接入之前应当对接入方案进行审核和安全评估，确认达到国家和行业网络安全要求并签订安全协议后方可授权接入网络。

第十五条 辖区单位重要生产信息系统应当与互联网及其他网络区域实行安全隔离，并根据承载业务对网络进行分区分域管理，在不同安全域间实施访问控制。

第十六条 辖区单位应当严格系统变更管理，建立系统重要变更审批程序，记录变更实施过程。

第十七条 辖区单位应当严格控制移动式设备接入、无线接入等网络接入行为，明确接入方式、访问控制等措施要求，形成网络接入日志并定期审计，确保未经审查通过的设备无法接入。

第十八条 在机场、航空器等公共场所为民航旅客提供互联网接入服务的企业，应当采取身份认证、上网行为审计等安全技术措施保护旅客个人信息安全，同时保证公共网络区域与单位内部网络物理隔离。

第十九条 辖区单位应当加强对服务器上的应用、服务、端口的安全管理，定期更新恶意代码库及系统补丁，定期实施漏洞扫描、恶意代码检测。

第二十条 辖区单位应当制定终端计算机管理制度，严格终端计算机的安全管理，采取集中管控、用户识别、访问控制、安全审计等技术防护措施。

第二十一条 辖区单位应当严格移动存储介质管理，防止移动存储介质在不同网络区域之间使用时造成恶意代码的传播和信息泄露。

第二十二条 辖区单位应当建设网站和网上运行业务系统技术防护体系，采取有效防护措施，提高防篡改、防病毒、防攻击、防瘫痪、防挂马等能力，定期进行安全检查和风险评估。

第二十三条 辖区单位应当建立重要系统和核心数据的容

灾备份制度，明确业务和系统的恢复目标以及相应的恢复预案，保证关键业务的连续性。重要网络设备和通信线路应当具有冗余备份。

第二十四条 辖区单位应当严格工作信息和业务数据的安全管理，不得在非涉密计算机及相关设备上处理、传递、转发涉密或敏感信息。

第二十五条 辖区单位应当建立网络安全信息通报制度，开展信息通报工作，不得瞒报、缓报、谎报、迟报和推诿责任。

属于较大以上网络安全事件的，按以下程序报告:

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，网络运营者应当第一时间向民航局人事科教司、管理局、所在地监管局、公安机关报告，最迟不得超过 15 分钟。

发生涉及关键信息基础设施的较大网络安全事件，网络运营者应当在 30 分钟内向管理局、所在地监管局、公安机关报告。

其他网络运营者应当及时向所在地监管局报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，应当第一时间向管理局、所在地监管局报告，最迟不得超过 1 小时。

属于一般网络安全事件的，网络运营者应该按照《民航网络与信息安全信息通报办法》进行报告。

第二十六条 报告网络安全事件时，应当包括下列内容:

（一）涉事单位名称及涉事系统或设施基本情况;

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果; 对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等;

（三）事态发展趋势及可能造成的进一步影响和危害;

（四）网络安全事件原因初步分析意见;

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等;

（六）拟进一步采取的应对措施以及请求支援事项;

（七）网络安全事件现场保护情况;

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第二十七条 辖区单位应当建立网络安全培训制度，定期开展网络安全意识教育与网络设备安全操作基础培训，对系统建设、运维人员和网络安全从业人员进行专项技能培训。

第二十八条 辖区单位应当建立网络安全责任追究制度，对违反网络安全管理要求的人员给予处理，并以适当方式对网络安

全事件及相关责任人进行通报。实施责任追究应当实事求是，分清集体责任和个人责任。对领导班子、干部员工进行问责时，各单位的网络安全和信息化领导机构办公室可以提出问责建议。

第二十九条 辖区单位应每年12月10日前将本单位网络安全第一责任人、直接责任人、责任部门负责人、联络员信息报送所在地监管局。监管局汇总后于当年12月20日前报管理局。

第三十条 辖区单位应每年12月10日前将本单位的网站和信息系统、关键信息基础设施的基本信息建立名录后报送所在地监管局。监管局汇总后于当年12月20日前报管理局。

第三十一条 辖区单位应当建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，考核结果送干部员工主管部门，作为对领导班子和干部员工综合考核评价的重要内容。

第四章 网络安全等级保护

第三十二条 辖区单位是信息系统安全等级保护的责任主体，应当依照本办法及国家和民航相关标准规范，履行信息安全等级保护的义务和责任。

第三十三条 网络安全等级保护坚持“自主定级、自主保护、重点保护、同步建设、动态调整”的原则，实行统一领导、分级管理、分工负责的管理体制。

第三十四条 信息系统的安全保护等级应按照民航相关标

准、规范、指南等，根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。新建信息系统或者信息系统发生重大变更时，应当首先确定信息系统的安全保护等级，并同步建设符合该安全保护等级要求的安全保护设施。

第三十五条 确定信息系统安全保护等级时，一般按照确定定级对象、初步确定等级、专家评审、主管部门审批、公安机关备案审查、最终确定级别等步骤进行。专家评审时，专家组最低由三名信息安全专家和业务专家组成，其中一名应为等级保护高级测评师。在组织专家评审时，专家组要对定级是否合理形成相关意见建议。

第三十六条 信息系统安全保护等级确定后，辖区单位应在三十日内向所在地公安机关办理备案手续。同时，将定级结果和备案证明材料报送所在地民航行政管理机构。

第三十七条 辖区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，建设符合该等级要求的信息安全设施，制定并落实符合系统安全保护等级要求的安全管理制度，使用符合国家有关规定、满足信息系统安全保护等级需求的信息技术产品。三级以上信息系统的安全保护技术措施应符合“一个中心、三重防护”的体系架构，涵盖安全物理环境、安全通信网络、安全区域边界、安全计算环境及安全管理中心等多个方面。

第三十八条 信息系统建设完成后，辖区单位或其主管部门应当选择符合国家要求的测评机构，定期对信息系统安全等级状况开展等级测评。第二级信息系统应当每两年进行一次等级测评；第三级信息系统应当每年至少进行一次等级测评；第四级信息系统应当每半年至少进行一次等级测评；第五级信息系统应当依据特殊安全需求进行等级测评。辖区单位应当定期对信息系统安全状况开展风险评估。

实施等级保护测评的机构应当具备国家认可的信息安全等级保护测评资质。

第三十九条 辖区单位在经测评或自查发现信息系统安全状况未达到安全保护等级要求时，应当制定方案进行整改。整改完成后，应将整改报告向所在地监管局和公安机关备案，并接受监督检查。

第五章 关键信息基础设施保护

第四十条 管理局根据民航局制定的认定规则负责组织新疆民航的关键信息基础设施认定工作，相关材料及时报民航局，将民航局认定结果通知关键信息基础设施运营者，并通报公安机关。

第四十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当在两个月内将相关情况报告管理局。管理局自收到报告之日起三个月内组织重新认定工作，相关材料及

时报民航局，将民航局认定结果通知运营者，并通报公安机关。

第四十二条 关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第四十三条 关键信息基础设施运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

第四十四条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责（包括但不限于）：

（一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对关键信息基础设施设计、建设、运行、维护等服务

实施安全管理;

（八）按照规定报告网络安全事件和重要事项。

第四十五条 关键信息基础设施运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第四十六条 关键信息基础设施运营者应当每年初制定关键信息基础设施安全保护计划，报管理局批复后实施。

第四十七条 关键信息基础设施运营者应当优先采购安全可信的网络产品和服务;采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第四十八条 关键信息基础设施运营者采购网络产品和服务,应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第四十九条 关键信息基础设施运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第五十条 关键信息基础设施运营者发生合并、分立、解散等情况，应当及时报告管理局，并按照管理局的要求对关键信息基础设施进行处置，确保安全。

第六章　网络安全信息管理

第五十一条　辖区单位使用网络应当遵守法律法规，遵守公共秩序，尊重社会公德，维护国家利益和民族团结，不得利用网络从事《新疆维吾尔自治区网络安全管理条例》禁止的活动。

第五十二条　辖区单位应当建立完善网站、公众号、服务号等互联网信息发布审核制度，确保发布的信息内容安全。

第五十三条　辖区单位应当依照法律法规的规定，落实网络信息内容的安全技术防范措施，防止本办法第五十二条中所列禁止利用网络从事活动的信息在本单位的网络信息系统上传播。如果发现有此类情况，应当立即停止网络信息系统的运行，保存相关记录，删除相关信息，并及时按照规定报告。

第五十四条　辖区单位不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。

第五十五条　辖区单位所收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第五十六条　辖区单位应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。未经被收集者同意，不得向他人提供个人信息，但经过处理无法识别特定个人且不能复原的除外。

第五十七条 辖区单位在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户，并按照要求向各监管局报告，监管局向管理局报告。

第五十八条 辖区单位应当建立生产运营信息共享管理制度，对于法律法规、规章和政策要求共享的生产运营信息予以安全保护。信息提供单位应当与信息获取单位签订信息使用和信息安全保护协议，明确信息共享内容、使用期限以及双方的权利、义务和责任。

第五十九条 辖区单位的重要信息系统在境内运营中收集和产生的个人信息和重要数据应当在境内存储。

第七章 网络安全监督检查

第六十条 管理局、各监管局应当依照国家和行业要求，实行网络安全年度检查和专项检查制度，将网络安全检查工作列入年度行政检查计划，并组织落实国家和行业布置的其他检查工作。

第六十一条 新疆民航各级行政管理机构在履行网络安全监督管理职责时，应当加强与自治区网信部门、公安机关等部门的工作协同与信息共享，建立健全跨部门协作机制，共同维护网络安全。

第六十二条 新疆民航各级行政管理机构在年度或专项检查中应当按照民航局有关要求，记录检查结果，提出处理意见。

被检查单位根据处理意见进行整改。

第六十三条 新疆民航各级行政管理机构对检查中发现的重大安全隐患，应当责令有关单位立即排除；对检查中发现的安全管理缺陷或安全隐患，应当向有关单位提出限期整改要求；对检查中发现的违法行为，应当立即制止，依法处罚。

第六十四条 被检查单位应当配合检查，对检查中发现的问题进行整改后，将整改情况上报组织检查的新疆民航行政管理机构。

第六十五条 辖区单位应按照民航局有关要求建立自查制度，制定自查计划，开展法定自查。

第六十六条 管理局和监管局网络安全监察员依法履行下列职责：

（一）依照本规定对辖区内民航各企事业单位网络安全工作实施监督检查；

（二）按照网络安全信息通报制度向上级行政管理机构报告辖区内网络安全情况；

（三）参与辖区内网络安全事件调查；

（四）依法处理辖区内民航各企事业单位违反国家和行业网络信息安全法律、法规和规章的行为；

（五）承办法律、法规或规范性文件规定的或上级交办的其他工作。

第六十七条 网络安全监察员参加强化通识培训和强化业

务培训时间不少于民航局规定要求。

第八章　网络安全应急管理

第六十八条　辖区单位应当建立网络安全应急管理制度，设立或者指定应急工作管理机构，负责应急管理工作。

第六十九条　辖区单位应当制定网络安全事件应急处置预案，定期开展应急演练，并对演练情况进行评估，针对演练中发现的问题，补充修订应急预案。

第七十条　辖区单位应当根据实际需求与当地电信、电力、公安等部门建立应急协调机制。

第七十一条　辖区单位在发生网络安全事件时，应当按照《新疆民航处置网络安全事件专项应急预案》及本单位制定的应急预案及时进行处置，并按照规定进行通报。

第七十二条　辖区单位因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第九章　附则

第七十三条　辖区单位构成违反《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等法律、行政法规的行为的，管理局、各监管局可依法依规进行相应的处罚。

第七十四条 本办法由民航新疆管理局负责解释。

第七十五条 本办法自发布之日起30日后正式施行。原《民航新疆网络安全管理暂行办法》（新管局发〔2019〕30号）同时废止。