中国银保监会办公厅文件

银保监办发〔2018〕50号

中国银保监会办公厅关于加强无线网络安全管理的通知

各银监局，各保监局，各政策性银行、大型银行、股份制银行，邮储银行，外资银行，金融资产管理公司，各保险集团（控股）公司、保险公司、保险资产管理公司、保险专业中介机构：

近年来，无线网络技术发展较快，在银行保险机构的业务服务、移动办公和互联网接入等领域得到广泛应用，但由于缺乏线路连接控制及管理不规范问题，无线网络信息截取、非法入侵、伪冒诈骗等风险近期呈上升态势。为加强风险防范，确保银行业和保险业网络和信息系统安全，现就加强无线网络安全管理有关事项通知如下：

一、本通知所指无线网络，指以无线电波为信息传输媒介，运用无线通讯技术实现数据传输的网络，包括银行保险机构的无线局域网（简称“WLAN”）和其使用的专用移动通讯网。主要无线网络类型包括：

（一）利用运营商提供的3G/4G等专用移动通讯网，支持离行金融机具、移动业务终端等设备连接银行保险机构内部通讯网络，或经营场所间网络通讯的移动通讯网络（简称“移动通讯专网”）。

（二）接入银行保险机构内部通讯网络，支持业务经营、办公、开发测试、培训等的无线局域网络（简称“内网WLAN”）。

（三）为银行保险机构客户或员工提供互联网服务的无线局域网络（简称“互联网WLAN”），包括自建、租用运营商的互联网WLAN等。

二、银行保险机构应充分认识无线网络安全风险，在无线网络建设中安全技术措施应遵循“同步规划、同步建设、同步使用”的原则同步推进，严格禁止私搭乱建和未经授权使用无线网络，杜绝不符合规范的无线网络。境外分支机构还应遵守所在国家和地区的监管要求和法律规定。

三、银行保险机构应明确对无线网络安全管理的职能部门，建立无线网络管理制度和技术安全规范，要按照“谁主管谁负责、谁运营谁负责”的原则，建立无线网络的审批备案管理制度，对使用需求、访问权限和用户行为进行严格管理。

四、银行保险机构应将无线网络安全管理纳入日常信息科技

风险评估、检查及审计范围，检查和评估各级部门无线网络使用的合规性、安全性、管理有效性。

五、银行保险机构应采取以下措施，控制无线网络安全风险。

（一）银行保险机构的无线网络应划分独立网段或虚拟局域网，进行安全隔离和访问控制，防止非授权访问。“互联网WLAN”应与内部网络实施严格隔离，并通过技术措施控制与内部网络的通讯。

（二）银行保险机构WLAN应通过绑定设备序列号或MAC地址（硬件地址）等硬件特征信息对无线接入点进行准入控制，合理设置传输功率，控制无线信号的覆盖范围。

（三）“内网WLAN”网络名称（简称SSID）应采用规范的命名规则，命名应尽可能不泄露所属银行保险机构、网络特性、物理位置等信息，禁止使用缺省的SSID。生产环境“内网WLAN”应禁止使用SSID广播，避免攻击者通过扫描直接获取无线网络信息。

（四）银行保险机构应采用安全、可靠的加密协议，对无线通信信道进行安全加密，以保证“内网WLAN”和“移动通讯专网”传输信息的保密性、完整性，防止信息被非法窃听、伪造、篡改或重放。

（五）银行保险机构应确保无线网络设备的物理安全，并采取安全基线管理措施，启用必要的安全设置，禁用不必要的服务，强化无线网络设备的管理账号和口令安全，禁止使用弱口令。

（六）银行保险机构应加强无线网络用户管理，防止非法用户访问；“内网WLAN”应禁止共享账号，并采用双因素认证方式对

接入用户进行身份校验，应停用长时间未活动用户；“互联网WLAN”应通过短信验证码、微信或用户名/密码等方式对接入网络的用户进行实名认证，对接入设备的网络访问进行监测，并加强用户密码安全管理。

（七）“内网WLAN”的接入终端应经过审批授权，采取无线网络终端设备准入控制措施，防止终端通过WLAN非法接入银行保险机构内部网络；禁止操作系统管理权限被非法破解的终端设备接入“内网WLAN”。银行保险机构应采取措施控制移动智能终端（如平板电脑、手机等）在内网和互联网间交叉使用的风险，加强应用安全和数据泄露防护，防范恶意代码传播。

（八）“移动通讯专网”应使用双因素认证方式，通过专用SIM卡、用户名/密码、证书等，对移动终端、离行机具等设备进行认证，保障无线设备接入安全。

（九）银行保险机构应采用防火墙、入侵检测、防病毒等网络安全技术措施，并加强对伪冒WLAN热点的侦测，防范欺诈、钓鱼等无线网络攻击。

（十）银行保险机构短期使用、临时搭建的无线网络，应遵循前述无线网络安全管理和技术规范要求，并须明确使用期限，期满后应及时拆除或关闭。

（十一）对于不涉及保密信息和敏感数据，且不与银行保险机构内部网络或互联网连接的“孤岛”临时性无线网络，其安全管理参照前述要求执行。

六、银行保险机构应对无线网络安全威胁进行持续监控，及

时处置无线网络安全事件，防止无线网络感染和传播病毒等恶意程序，防范无线网络遭受入侵和攻击风险。

（一）银行保险机构应收集无线网络设备、相关安全设备的日志信息，分析和监测网络攻击事件。

（二）银行保险机构应建立网络安全事件的应急响应机制，制定专项应急预案及现场处置方案，明确处置流程，确保无线网络安全事件得到有效处置。发生重大网络安全事件时，应按照监管隶属关系，及时向中国银保监会或其派出机构报告。

七、银行保险机构应加强无线网络安全漏洞发现与处置，每年开展安全风险评估和测试，针对网络部署架构、设备和系统，积极采取配置检测、漏洞扫描、渗透测试等技术手段，及时发现和修复无线网络安全漏洞，定期开展模拟无线网络攻击应急演练。

八、银行保险机构委托外部服务商代为提供无线网络服务时，应明确外包服务商的安全责任，要求其每年提供无线网络安全风险评估报告，并督促其进行问题整改。

九、银行保险机构应积极开展无线网络用户安全意识教育，严格要求内部员工遵守网络与信息安全管理规定，在内网 WLAN 和移动通讯专网的移动终端中，禁止安装和使用无线网络密码分享等有危害性的应用程序；供银行保险机构客户使用的“互联网 WLAN”，应在营业网点显著位置发布无线网络的使用提示，防止用户接入假冒无线网络。

十、各银行保险机构应迅速开展一次全面自查工作，对本机构的无线网络进行全面梳理，建立无线网络台账；对照本通知要

求，开展无线网络安全风险评估，重点就无线网络的规划建设、运行监控、漏洞管理、安全审计等领域进行自查、评估，对发现的问题立即进行整改，确保无线网络安全。各机构应于2018年8月31日前完成自查工作，按照监管隶属关系，向中国银保监会或其派出机构提交自查和风险评估报告。请各银监局和各保监局分别汇总辖内银行业金融机构和保险专业中介机构的自查和风险评估报告，各保险集团公司汇总下属各子公司自查和风险评估报告，于2018年9月15日前报送中国银保监会。

联 系 人：刘洋　张金棋　张伟

联系电话：(010)66278548　66278611　66286569

电子邮箱：liuyang_d@cbrc.gov.cn

zhangjinqi@cbrc.gov.cn

wei_zhang@circ.gov.cn

中国银行保险监督管理委员会办公厅

2018年6月12日

（此件发至银监分局、保监分局和地方法人银行业金融机构，请各保监局转发至辖内保险专业中介机构）

公开属性：不予公开

内部发送：原银监会信科部、政研局、审慎局、检查局、法规部、普惠部、创新部、消保局、政策银行部、大型银行部、股份制银行部、城市银行部、农村金融部、外资银行部、信托部、非银部，原保监会统信部、发改部、政研室、消保局、财险部、人身险部、中介部、资金部、法规部。（共印20份）

联系人：刘　洋　　联系电话：66278548　　校对：骆絮飞

中国银行保险监督管理委员会办公厅　　2018年6月13日印发