保险机构信息化监管规定
（征求意见稿）

第一章　总　则

第一条[制订目的]为了加强对保险机构信息化工作的监督管理，促进信息化工作规范化与标准化建设，有效防范和化解新技术风险，切实维护保险业信息安全，根据《中华人民共和国保险法》、《中华人民共和国计算机信息系统安全保护条例》等法律、行政法规，制定本规定。

第二条[适用范围]本规定适用于在中华人民共和国境内依法设立的保险机构，包括保险集团（控股）公司、保险公司和保险资产管理公司。

第三条[名词释义]本规定所称保险机构信息化，是指保险机构将计算机、通信、网络等现代信息技术，应用于业务交易处理、经营管理和内部控制等方面，持续提高运营效率、优化内部资源配置和提升风险防范水平的过程。

信息化工作内容包括建立健全信息化治理机制、制定实施信息化管理制度、规划建设信息化基础设施、采购开发信息化系统，以及建立相应的安全保障体系等。

第四条[基本原则]保险机构信息化工作要遵循安全性、可靠性和有效性相统一的原则，坚持信息化战略与业务战略相融合、技术路线与科技发展方向相一致、应用系统与管理需求相适应的

基本要求，统筹规划本机构的信息化工作，处理好安全与发展、安全与建设、安全与运营的关系，保障本机构信息系统安全稳定持续运行。

第五条[执行标准]保险机构信息化工作应当符合国家有关规定和中国保险监督管理委员会（以下简称中国保监会）的要求。

保险机构是信息化工作的责任主体。保险机构法定代表人对本机构信息化工作承担首要责任。

第六条[监督管理]中国保监会依法对保险机构的信息化工作实施监督管理。

第二章　信息化治理

第七条[名词释义]信息化治理是指保险机构通过明确有关信息化决策权归属机制和信息化责任承担机制，合理利用信息化资源，达到推动业务发展、促进收益最大化等战略目标的过程。

第八条[董事会职责]保险机构董事会应当履行以下信息化工作管理职责:

（一）贯彻国家信息化工作的法律、行政法规、技术标准和中国保监会的要求;

（二）审查批准本机构信息化工作战略规划，确保与总体业务战略和重大策略相一致;

（三）建立分工合理、职责明确、相互制衡、报告关系清晰的信息化治理组织架构;

（四）保障信息化工作所需资金;

（五）掌握公司主要的信息化工作情况，审阅并向中国保监会报送信息化工作年度报告;

（六）强化本机构人员的信息化意识和信息安全意识，加强信息技术专业队伍建设，建立人才激励机制;

（七）保障内部审计部门进行独立有效的信息化工作审计，对审计报告进行确认并组织整改;

（八）确保本机构涉及客户、账务，以及产品等信息的核心系统在中华人民共和国境内独立运行，并保持最高的管理权限，符合中国保监会监管和实施现场检查的要求;

（九）及时向中国保监会报告本机构发生的重大信息安全事故或者突发事件，按相关预案快速响应;

（十）配合中国保监会做好信息化工作监督检查，并按照监管意见进行整改;

（十一）国家相关部门、中国保监会要求的其他信息化工作。

第九条[信息化工作委员会]保险机构应当设立由董事会直接领导管理下的信息化工作委员会。信息化工作委员会主任由董事长、总经理或者执行董事担任，成员应当包括首席信息官、信息技术部门和主要业务部门代表。

信息化工作委员会有权向董事会直接报告和提出建议。由其负责承办董事会交办的信息化工作事项并监督落实，并定期向董事会和高级管理层汇报信息化工作整体情况。

第十条[首席信息官]保险机构应当设立首席信息官。首席信

息官直接对信息化工作委员会主任负责，参与本机构决策。首席信息官、信息化工作委员会主任对信息化工作承担主要责任。

首席信息官的职责包括:

（一）直接参与本机构信息化工作有关的业务发展和经营管理决策;

（二）推动信息化战略规划纳入本机构全面发展框架，信息系统开发战略规划应当符合本机构的总体业务战略规划和风险管理策略;

（三）负责信息技术部门的领导与管理，承担本机构的信息化工作职责;

（四）负责建立健全信息化制度规则体系;

（五）保障信息化工作管理的有效性，并使有关管理措施落实到内设部门和分支机构;

（六）组织公司专业培训，提高人才队伍的专业技能;

（七）履行国家相关部门、中国保监会要求的其他信息化工作职责。

第十一条[任职条件]保险机构首席信息官应当由本机构董事会成员或者高级管理人员担任，并应当具备以下条件:

（一）具有诚实信用的职业操守、良好的合规意识，具备履行职务必需的知识结构和专业技术能力;

（二）从事信息技术工作五年以上，且在金融机构工作三年以上; 或者其他足以证明其具有拟任职务所需知识、能力、经验的职业经历。

第十二条[信息技术部门]保险机构应当设立信息技术部门，统一负责本机构信息化工作规划、建设、管理和运行维护等，承担本机构信息化工作委员会日常工作。

第十三条[明确职责]保险机构应当明确本机构内设部门及分支机构信息化工作职责，并加强指导与监督。

第十四条[规划制订]保险机构应当建立信息化规划的制定、实施、评估和修订的工作机制。根据公司业务发展战略，制定明确的中长期信息化规划，规划期为三至五年。

规划的制定、实施、修订应当由本机构信息化工作委员会提交董事会审议批准。

第十五条[执行机制]保险机构应当制定明确的信息化工作制度，明确实施标准和操作流程，及时更新、发布。

保险机构应当根据公司总体业务规划和信息化工作需要，制定专门的信息化经费预算，确保资金投入，有效支持业务发展。

保险机构应当制定有利于公司可持续发展的信息化人力资源政策，健全信息技术专业人才激励机制，合理配备信息技术人员，并定期对信息技术人员和公司其他人员分别开展专业技术培训。

第十六条[内部审计]保险机构应当在内部审计部门设立专门的信息化风险审计岗位，配备足够的资源和具有专业能力的信息化工作审计人员，对本机构信息化工作进行全面、独立审计。

第十七条[集团管理]保险集团（控股）公司根据自身总体业务规划和风险管控要求，可以对各子公司信息化工作实行集中管理，但各法人机构之间的信息系统、原始数据等应当有效隔离，

并各自承担信息安全风险管理责任。

保险集团（控股）公司和子公司依法对信息安全关联风险事故承担责任。

第三章　信息系统建设与运行维护

第十八条[架构规划]保险机构应当根据本机构的总体业务发展战略和信息化风险管理策略，对信息系统建设与运行维护进行总体规划，加强各信息系统之间的集成与整合，实现财务、业务等核心系统的无缝对接，促进经营管理流程信息化，满足保险监管数据采集要求和保险业信息共享需要。

第十九条[制度框架]保险机构应当建立完善的信息系统管理组织，制定覆盖信息系统全生命周期的管理制度、技术标准和操作规范，保障信息系统规划、建设和运行维护各项工作的安全实施。

第二十条[安全定级]保险机构应当根据国家信息安全等级保护有关规定和所涉信息对机构经营管理的重要程度，合理确定信息系统的安全等级，并按照相应等级要求对信息系统进行等级测评、安全建设和运行维护。重要信息系统定级情况应当根据国家有关规定和中国保监会要求进行备案。

第二十一条[开发形式]保险机构应当增强信息系统的自主研发能力。根据自身情况，信息系统开发还可以采取合作开发、定制开发和外包开发等形式。

对合作开发和外包开发，保险机构应当通过合同约定源代码所有权归属，确保拥有合理的源代码使用授权或者所有权，严格防范合作开发商或者外包商终止服务导致的风险。

第二十二条[开发测试]保险机构信息系统的开发测试应当与生产管理严格分离，不得使用未脱敏的生产数据用于开发、测试环境。严格限制开发人员访问源代码的权限，并保障核心系统开发实施安全。

信息系统正式上线运行前，应当对其功能、性能及安全性进行测试。核心系统应当通过第三方测试机构测试,本机构具有独立测试团队的，也可以由该独立测试团队测试；面向互联网应用的系统还应当通过第三方安全测试。信息系统的重大改造升级应当按照新信息系统建设标准进行测试。

信息系统经测试合格，并由本机构信息技术部门和业务部门共同批准后方可上线运行。

第二十三条[系统运行维护]保险机构应当建立完善的信息系统运行维护管理流程，清晰界定信息技术部门和业务部门的运行维护职责，并按照下列要求建立信息系统的身份鉴别、权限分配、操作日志、故障处理规范:

（一）按照等级保护要求建立相应的身份鉴别机制;

（二）严格规范账号权限分配、使用和回收管理流程;

（三）信息系统运行维护操作日志应当按照国家有关要求和业务经营需要进行分类保存;

（四）建立信息系统故障全面记录、分析和解决机制。

第二十四条[系统变更与数据迁移、修改]信息系统变更和数据迁移时，应当制定合理的技术方案，充分测试，做好备份，保证信息系统及数据安全。严格控制后台修改系统数据，确需修改的要做到事前批准、事中监控和事后留痕。

第二十五条[安全防护]保险机构应当按照下列要求建立健全信息系统备份及灾难恢复、防病毒、密码管理、入侵检测、系统日志等安全管理机制:

（一）根据数据及系统的重要性，明确数据及系统的备份与灾难恢复策略;

（二）加强密码设备及使用人员管理，使用符合国家标准和加密要求的技术和产品;

（三）采取恶意代码防范措施，确保具备主动发现和有效阻止恶意代码传播的能力;

（四）信息系统日志在保存期限内内容不得删除、修改或者覆盖，并实现对关键岗位、异常操作等高风险因素的记录。

第二十六条[互联网应用]保险机构应当按照下列要求加强对门户网站、社交网络公众账号等互联网应用系统的管理:

（一）根据国家有关规定备案;

（二）建立网站信息发布审批制度，严格控制网站内容发布权限;

（三）加强技术保障和运行监控，保障网络交易安全和交易记录可追溯。

第二十七条[文档完备]保险机构的重要信息系统有关资料和

信息系统的重要信息应当按照中国保监会要求备案。

保险机构要建立覆盖信息系统全生命周期的文档管理体系，确保文档记录完整、及时、有效。

第四章　基础设施建设与保障

第二十八条[基础设施]基础设施指保障信息系统运行的物理环境，主要包括数据中心和网络资源。

本规定所称数据中心包括生产中心和灾难备份中心（以下简称灾备中心）。

生产中心是指保险机构对全部业务、客户和管理等重要信息进行集中存储、处理和维护，具备专用场所，为业务运营及管理提供信息化支撑服务的组织。

灾备中心是指保险机构为保障其业务连续性，在生产中心故障、停顿或者瘫痪后，能够接替生产中心运行，具备专用场所，进行数据处理和支持重要业务持续运行的组织。

灾备中心同城模式（以下简称同城灾备）是指灾备中心与生产中心位于同一地理区域，一般距离数十公里，可防范火灾、建筑物破坏、电力或者通信系统中断等事件。灾备中心异地模式（以下简称异地灾备）是指灾备中心与生产中心处于不同地理区域，一般距离在数百公里以上，不会同时面临同类区域性灾难风险，如地震、台风和洪水等。

本规定所称网络资源是指支撑系统运行的网络专线、网络带

宽、网络地址、网络域名以及相关网络设备等虚拟及物理设施。

第二十九条[规划设计]保险机构应当以本机构业务总体规划为根本,围绕数据资产的管理和应用,科学规划数据中心的总体架构和实施路线，保证网络、数据、应用、安全各要素有机结合。

数据中心规划应当报中国保监会备案。

第三十条[建设时间]保险机构在筹备时，应当按照中国保监会规定的信息化建设准入标准设立生产中心。生产中心运行五年内建立灾备中心，灾备中心的建设与管理必须达到中国保监会规定的标准。

保险机构应当不断完善生产中心、同城灾备、异地灾备的灾难备份体系，逐步实现更高安全水平的信息系统运行模式，切实提高防灾减灾能力，保障业务连续性。

第三十一条[建设标准]保险机构可以采取自建、共建、外包的方式设立数据中心，数据中心的机房设计标准必须符合国家标准规范和中国保监会的要求。

数据来源于中华人民共和国境内的，数据中心的物理位置应当位于境内。

第三十二条[人员管理]保险机构应当指定专门机构和专业队伍负责数据中心运营与管理，明确数据中心各岗位人员职责，建立完善运行指标体系和服务评价体系，保证运行维护队伍人员稳定、工作高效。

第三十三条[管理制度]保险机构应当建立健全并严格执行数据中心管理制度、技术规范、操作指南，包括机房管理、运行管

理、设备管理、数据管理、应急管理等。

第三十四条[安全管理]保险机构数据中心应当设置安全工作机构，加强人员安全、物理环境安全、设备资产安全、操作安全、运行维护安全、链路安全、网络安全及应用安全等方面的安全管理。

第三十五条[设施监控]保险机构应当对信息化基础设施实施有效监控。数据中心基础设施安全防护和保障应当按功能区域划分安全控制级别，不同级别区域采用独立的出入控制设备并集中监控。应当对基础设施设备、机房环境状况、安全防护系统状况实行 7×24 小时实时监测。深入应用自动控制、虚拟化管理等新技术，提高监控水平和效率。

第三十六条[网络规划]保险机构网络资源应当满足高性能、高可用性、高安全性、可扩展性等要求，为信息系统提供安全、稳定、高效的运行环境。数据中心应当用两条或者多条通信线路互为备份，互为备份的通信线路不得经过同一路由节点。

第三十七条[外联管理]保险机构内部网络与保险中介机构、第三方机构等外联单位网络连接时，应当明确网络外联种类方式，采用可靠连接策略及技术手段，实现彼此有效隔离，并对跨网络流量、网络用户行为等进行记录和定期审计。

第五章　外包管理

第三十八条[名词释义]本规定所称外包是指保险机构将本机

构信息化工作委托给服务提供商进行处理的行为，包括咨询外包、系统建设外包、系统运行维护外包、基础设施外包和信息安全外包等。

第三十九条[建立制度]保险机构实行信息化工作外包，应当制定完备的外包服务管理制度和风险评估机制，确保有效应对和处置外包风险。

第四十条[审慎要求]保险机构应当根据涉及信息资产的关键性和敏感程度，审慎确定外包服务范围。信息系统安全管理责任不得外包。

下列外包实施前应当经过本机构董事会批准，并按照中国保监会要求报告:

（一）保险机构对数据中心等基础设施实施的整体外包;

（二）对涉及国家安全、本机构商业秘密，以及客户隐私等敏感内容的信息系统外包。

第四十一条[外包资质]保险机构应当根据不同的外包业务要求，优先选用具备信息安全管理体系认证资质的信息技术服务机构提供外包服务。数据中心外包服务提供商应当符合本规定第四章所规定的标准和要求。

第四十二条[外包合同]保险机构与外包服务提供商签订书面外包服务合同，合同应当包括外包服务范围、安全保密、知识产权、业务连续性要求、争端解决机制、合同变更或者终止的过渡安排、违约责任等条款。

保险机构必须要求外包服务提供商承诺接受和配合中国保监

会对保险机构信息化工作相关的现场检查和日常监督。

第四十三条[分包要求]保险机构要严格控制外包服务提供商的转包和分包行为。对于确有第三方外包服务提供商参与实施的项目应当采取严密措施，保证外包服务质量和安全不受影响。

第四十四条[外包监督]保险机构应当加强外包服务提供商及其服务人员的管理，与外包服务提供商建立起有效的信息交流与沟通机制，保证外包服务人员的相对稳定。

第四十五条[股东影响]保险机构信息化建设和管理与其非保险类股东有重大关联的，保险机构信息化治理与规划、业务、财务等核心系统和重要数据信息及其管理必须保持独立完整。其他信息化事项外包给股东的，按照本规定外包要求实施管理。

第四十六条[购买保险]保险机构应当优先选择购买相应商业保险的外包服务提供商，以保障安全事件发生时外包服务提供商有足够的经济赔偿能力。

第四十七条[定期评估]保险机构应当建立评估考核机制，定期对外包服务提供商的财务状况、技术实力、安全资质、风险控制水平和诚信记录等进行审查、评估与考核，确保其设施和能力满足外包要求。

第六章　信息安全管理

第四十八条[信息安全]本规定所称信息安全是指利用信息技术及管理手段，保护信息在采集、传输、交换、处理和存储等过

程中的可用性、保密性、完整性和不可抵赖性。

信息安全包括网络安全、系统安全和内容安全，涵盖物理环境、网络、主机系统、桌面系统、数据、应用、存储、灾备、安全事件管理、人员等各层面安全。

第四十九条[基本要求]保险机构要将信息安全置于信息化工作的首位，按照“积极防御、综合防范”的原则，加强信息安全与信息系统的同步规划、同步建设和同步使用，加强风险管理与控制，充分利用管理机制和技术手段，增强安全防护能力，构建完善的信息安全保障体系，确保重要信息系统持续稳定运行，保障业务活动的连续性。

第五十条[机构职责]保险机构应当按照“谁主管、谁负责，谁运营、谁负责，谁使用、谁负责”的原则，明确信息安全责任，强化安全意识，加强安全管理，全面落实信息安全管理责任制。

保险机构法定代表人对本机构信息安全承担首要责任，首席信息官、信息化工作委员会主任对本机构信息安全承担主要责任。

保险机构应当在信息技术部门设置专门机构，并配备足够具有专业知识和技能的专职人员，履行以下安全职责:

（一）贯彻落实国家和中国保监会有关信息系统安全管理的法律、行政法规、技术标准和相关要求;

（二）组织公司信息系统安全规划与建设工作，制定相关管理规定;

（三）组织制定信息化风险管理制度，建立风险识别、计量、监测和控制体系;

（四）建立有效的信息系统安全保障体系并定期或者根据工作需要及时进行检查、评估、改进、监控等工作;

（五）对信息系统安全事件进行管理、处置和上报;

（六）组织公司员工信息系统安全教育与培训;

（七）开展与信息系统安全相关的其他工作。

第五十一条[制度体系]保险机构应当建立完善的信息安全分类和保护制度体系，明确系统管理、网络管理、安全管理等岗位职责、管理权限和技能要求，细化工作流程，建立有效的执行机制、评估机制和监督机制。制度体系包括以下内容:

（一）信息安全组织管理制度;

（二）信息化风险管理与控制制度;

（三）人员安全管理制度;

（四）数据安全管理制度;

（五）资产安全管理制度;

（六）物理与环境安全管理制度;

（七）访问控制管理制度;

（八）网络运行维护管理制度;

（九）系统开发与维护管理制度;

（十）业务连续性管理制度;

（十一）业务风险信息化管控制度;

（十二）信息安全事故管理制度;

（十三）信息化外包服务管理制度。

第五十二条[安全机制]保险机构应当构建完善的信息安全风

险控制策略。针对信息安全的各层面、各环节，建立职责明确的授权机制、审批流程，以及完备有效、相互制衡的内部控制体系，定期根据安全风险态势进行评审和完善。

第五十三条[安全可控]保险机构应当优先采购安全可控的硬件设备和软件产品，稳步推进安全可控产品应用；积极创造条件，提高关键业务系统的研发水平，不断增强保险机构信息化工作的安全可控能力。

第五十四条[密码应用]保险机构应当严格按照国家金融领域密码应用要求，逐步实现密码技术在电子保单及保险领域的全面应用。

第五十五条[正版化]保险机构应当切实提高软件正版化意识和知识产权保护意识。禁止复制、传播或者使用非授权软件。对本机构具有知识产权的信息产品，应当采取有效措施加以保护。

第五十六条[等级保护]保险机构应当按照国家和中国保监会信息系统安全规范、技术标准及等级保护管理要求，进行定级、备案、测评和整改，确保不同等级的信息系统具备相应的安全防护能力。

第五十七条[安全认证]保险机构需要申请信息安全管理体系认证的，应当按照国家有关规定及中国保监会要求，选择国家认证认可监督管理部门批准的机构进行认证，并与认证机构签订安全和保密协议。

第五十八条[数据安全]保险机构应当制定数据管理相关制度和流程，规范数据采集、传输、存储、交换、备份、恢复和销毁

等环节，采取加密等手段防范数据泄露，保障信息数据的合法、合规使用，做好数据恢复有效性测试，防范灾难发生时数据丢失风险。

外资保险机构信息系统所载数据移至中华人民共和国境外的，应当符合我国有关法律法规。

第五十九条［终端管理］保险机构应当根据安全管理有关规定对计算机、移动设备等各类终端分别制定安全管理制度，严格规范终端网络准入、安全策略、软件安装与卸载等管理。

第六十条[资产管理]保险机构要建立软硬件和数据资源等信息化资产管理制度，编制资产清单，明确资产管理责任部门与人员，规范资产分配、使用、存储、维护和销毁等行为，定期对资产清单进行一致性检查并保留检查记录。

第六十一条[介质管理]保险机构要制定介质分类管理制度，根据介质存储内容与重要性明确存储介质类型、存放技术指标、保存期限等，并定期检查介质中存储的信息是否完整可用。

重要备份介质应当异地存放。介质送出维修或者销毁时，应当保证介质信息预先得到审查并妥善处理。

对于存储客户隐私等涉密信息的存储介质，应当严格依据国家有关法律法规及中国保监会要求保存与销毁。

第六十二条[灾备恢复]保险机构应当加强信息系统灾难恢复管理，制定业务连续性规划，并定期进行演练，以确保出现无法预见的中断时信息系统仍能持续运行并提供服务。

第六十三条[应急管理]保险机构应当针对可能发生的信息安

全重大突发事件，建立和完善分类应急管理体系，与网信、公安、通信、电力等部门建立沟通机制，与业务系统、基础设备等服务厂商建立协同机制，对重大自然灾害、恶意破坏等合理划分应急响应等级，明确应急响应启动程序、处理流程、上报要求、预警机制等。

保险机构应当每年至少进行一次应急演练，针对演练中暴露出的风险隐患进行整改。

第六十四条[新技术安全]保险机构应当主动跟踪研究应用新兴信息技术，在推进业务创新的同时，提高信息安全防护能力，防范和控制新技术应用带来的新风险。

保险机构需要使用云计算服务的,要充分评估使用云计算服务的价值和风险。重点关注云计算提供商满足服务等级协定以及提供连续稳定云服务的能力，并充分考虑敏感数据在云计算平台上运行的安全性、所采取的安全控制措施的可靠性以及系统和数据迁移方案完善性等风险因素。

第七章　内部审计

第六十五条[审计要求]保险机构内部审计部门应当根据业务性质、规模和复杂程度，对相关信息系统及其控制的适当性、合规性和有效性进行独立于本机构日常活动的审计。

第六十六条[审计职责]保险机构信息化工作内部审计部门的职责:

（一）制定审计计划，检查和评估保险机构信息系统和内控机制的充分性和有效性;

（二）按照审计计划和要求完成审计工作;

（三）对信息安全或者其他特殊事项进行专项审计;

（四）检查、督促整改意见的落实情况。

第六十七条[范围与频率]保险机构应当根据业务性质、规模和复杂程度，信息技术应用情况，以及信息技术风险评估结果，决定信息化工作内部审计的范围和频率，但至少应当每两年进行一次全面审计。

第六十八条[内审参与]保险机构进行重要信息系统建设时应当要求内部审计部门参与监督。

第八章　外部审计

第六十九条[规定要求]保险机构应当根据法律、行政法规和中国保监会要求，定期委托具备相应资质的外部审计机构进行信息化工作外部审计。

第七十条[委托授权]在委托审计过程中，保险机构应当确保外部审计机构能够对本机构的硬件、软件、文档和数据进行检查，以发现信息系统存在的风险。

国家法律法规和中国保监会规定的重要商业、技术秘密信息不在检查范围。

第七十一条[审计频率]保险机构至少应当每两年进行一次外

部审计。

第七十二条[配合审计]保险机构实施外部审计前应当与外部审计机构进行充分沟通，详细确定审计范围，不得隐瞒事实或者阻挠审计。

第七十三条[保密要求]保险机构在委托外部审计机构进行外部审计时，应当与其签订保密协议，并督促其严格遵守法律法规，保守本机构的商业秘密和信息化风险信息，防止其擅自对本机构提供的文件资料进行修改复制或者带离现场。

第九章　监督管理

第七十四条[监管原则]中国保监会对保险机构信息系统实行分类、分级监督管理。

第七十五条[监管内容]中国保监会依法组织制定和推动执行保险业信息化标准，并根据保险业信息化风险状况，对保险机构进行信息化风险提示，督促保险机构采取针对性措施消除信息化风险隐患。

第七十六条[开业验收]保险机构设立时信息化建设应当达到中国保监会规定的准入标准和要求，且经过验收后方可对外营业。

第七十七条[非现场监管]保险机构应当按中国保监会要求定期报送信息化风险管理报表以及不定期报送专项临时报表。

中国保监会根据信息化风险管理报表情况对保险机构进行评价，相关监管指标纳入偿付能力监管体系，针对不同风险等级采

取相应的监管措施。

第七十八条[现场检查]中国保监会根据保险业信息化总体安全状况、保险机构信息化反映出的突出问题，可以组织现场检查，存在下列情形的保险机构可以作为重点检查对象:

（一）信息化建设存在重大安全隐患的;

（二）发生信息系统重大突发性事件的;

（三）违反中国保监会信息化重大事项报告有关规定的;

（四）对中国保监会信息安全检查中发现的严重信息安全隐患未采取措施进行整改或者整改不力的;

（五）违反合规性要求，逃避中国保监会或者有关部门检查和处罚，恶意对信息系统数据进行篡改的;

（六）在报送信息化各类报表数据中，存在严重误报、漏报、错报、迟报等行为，且屡错不改或者整改不力的;

（七）中国保监会认为有必要进行信息化重点检查的其他情形。

第七十九条[外聘审计]中国保监会认为必要时可指定具备相应资质的外部审计机构对保险机构信息化工作进行审计。外部审计机构根据中国保监会委托对保险机构进行审计时，应当出示委托书，并依照委托书规定的范围进行审计。

第八十条[审计报告]保险机构内部审计、外部审计应当按照中国保监会颁布的信息化审计规范标准和要求进行，且应当在每次审计结束后三个月内将审计报告报中国保监会备案。

第八十一条[渗透测试]中国保监会在对保险机构信息安全进

行检查时，可以委托具有相应资质的信息安全监测机构进行有针对性的风险渗透测试。保险机构应当根据中国保监会要求，委托具有相应资质的信息安全监测机构进行风险渗透测试，并针对产生的问题进行技术修正。

第八十二条[共同监督]对涉及信息化外包服务提供商信息安全监管的有关事项，中国保监会与国家信息安全有关部门建立监管合作机制，实施有效监督。

第八十三条[派出机构]中国保监会派出机构负责辖区内保险公司分支机构、保险资产管理公司分支机构信息化工作的监督管理。中国保监会派出机构可以参照本规定制定辖区内信息化工作监督管理办法。

中国保监会派出机构接受中国保监会委托开展辖区内保险集团（控股）公司、保险公司和保险资产管理公司信息化检查等工作。

第八十四条[集团分工]本规定实施后，保险集团（控股）公司与子公司有关信息化工作职责分工和责任落实情况，应当按照中国保监会要求备案，如有变化，及时报告。

第八十五条[处罚规定]保险机构违反本规定，中国保监会可以依法对保险机构及其相关责任人采取责令改正、监管谈话、出具监管函、通报等措施；情节严重的，依法给予行政处罚。

第十章　附　则

第八十六条　未设立董事会的保险机构由本机构高级管理层

承担本规定赋予董事会的职责。境外保险公司分公司视为保险机构管理。

第八十七条 保险中介机构信息化监管制度由中国保监会另行制定。

第八十八条 本规定由中国保监会负责解释。

第八十九条 本规定自 年 月 日起施行。中国保监会2009年12月29日发布的《保险公司信息化工作管理指引（试行）》（保监发〔2009〕133号）同时废止。