银行业保险业网络安全管理办法

（征求意见稿）

第一章　总　则

第一条　【目的和依据】

为加强银行业金融机构、保险业金融机构和金融控股公司（以下统称金融机构）网络安全监督管理，规范网络安全工作，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国保险法》《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条　【适用范围】

本办法适用于在中华人民共和国境内依法设立的金融机构，包括金融控股公司、政策性银行、商业银行、农村合作银行、农村信用合作社、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、信托公司、理财公司、金融资产投资公司、人身保险公司、财产保险公司、保险资产管理公司、保险集团（控股）公司、再保险公司、政策性保险公司、相互保险组织等。

外国银行分行、贷款公司、外国保险公司分公司、保险专业代理机构、保险经纪人等金融监管总局及其派出机构监管的其他机构参照适用本办法。

第三条　【工作目标】

金融机构应当遵守国家网络安全相关法律、法规和监管要求，统筹发展和安全，积极防御、综合防范，保障网络安全，维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，有效应对网络安全事件，防范网络违法犯罪活动。

第四条　【总体要求】

金融机构应当依法履行网络安全保护义务，建立网络安全治理架构，构建网络安全管理体系，开展网络安全风险管理，与业务连续性管理、外包风险管理、数据安全管理等体系机制有效衔接，将网络安全风险纳入全面风险管理，确保网络安全管理能力有效支撑业务安全稳健运行。金融机构应当将境内外分支附属机构网络安全工作纳入整体网络安全管理体系。

金融机构应积极配合公安机关、国家安全机关依法开展网络安全保卫、防范违法犯罪活动和监督检查,并提供必要技术支持和协助。

第五条　【实施主体】

国家金融监督管理总局及其派出机构依法对金融机构网络安全实施监管。

第二章　网络安全治理

第六条　【建立网络安全治理架构】

金融机构应当建立网络安全治理架构，明确网络安全工作职责，构建网络安全保障体系，健全决策、管理、执行和监督考核机制，落实网络安全资源保障。

第七条　【网络安全责任制】

金融机构应当建立网络安全责任制，党委（党组）、董（理）事会对网络安全管理工作负主体责任。金融机构主要负责人为网络安全第一责任人，分管网络安全的领导班子成员（高级管理人员）为直接责任人。金融机构应当明确各层级网络安全责任，明确违规情形和责任追究事项，落实问责处置机制。

第八条　【网络安全主管部门职责】

金融机构应当指定网络安全主管部门，负责本单位网络安全工作归口管理，履行以下网络安全职责:

（一）制定并组织落实网络安全规划、管理制度和操作规程;

（二）建立网络安全技术保障体系，采取有效的网络安全技术保障措施;

（三）统筹建立网络安全风险监测和事件应急管理机制，定期开展应急演练，主动识别网络安全风险，协调网络安全事件应急处置;

（四）设立网络安全团队，建设网络安全专业人才队伍，配备足够的人员，建立网络安全人才培养机制，开展网络安全技能培训；

（五）开展网络安全宣传教育，提升员工网络安全保护意识；

（六）按规定报告网络安全事件和重要事项；

（七）其他须统筹管理的网络安全工作事项。

第九条　【网络安全风险管理职责】

金融机构应当明确网络安全风险管理部门，并保持独立性。网络安全风险管理部门应制定并组织落实网络安全风险管理制度，建立网络安全风险识别、评估、计量、监测、报告机制，跟踪网络安全风险管理监管政策规定，并组织落实。

第十条　【网络安全审计职责】

金融机构审计部门负责网络安全审计，制定网络安全审计计划，开展网络安全审计工作，提出整改意见，并推动整改落实。必要情况下，可委托第三方机构对网络安全进行审计和评价，并向金融监管总局或者其派出机构报送外部审计报告。

第十一条　【监督考核与问责机制】

金融机构应当建立网络安全考核奖惩机制，定期对网络安全责任落实情况进行考核，并纳入单位年度考核体系。

第十二条　【网络安全文化建设】

金融机构应当培育良好的网络安全文化，常态化开展网

络安全宣传教育，每年至少开展一次全员网络安全培训，提高员工网络安全保护意识和水平。

第三章　网络安全建设和运行管理

第十三条　【网络安全建设规划】

金融机构应制定符合业务和科技发展需要的网络安全建设规划，网络关键节点、重要电力及通信线路、重要设备设施应当采取冗余备份措施，网络带宽和设备性能应当能够满足业务高峰期需求，应当确保网络安全保护措施与信息化建设“同步规划、同步建设、同步使用”。

第十四条　【制度体系】

金融机构应当建立与自身业务规模、复杂程度和风险水平相适配的网络安全管理制度体系，涵盖网络建设与运行，网络风险评估与监测预警、应急处置与业务连续性管理、供应链安全审查等关键环节，并定期评估优化。

第十五条　【物理安全管理】

金融机构应当合理选择数据中心物理位置，采取充分的物理安全保护措施，构建多层访问控制和监测预警体系，保障机房环境和设备安全可控。

第十六条　【资产安全管理】

金融机构应全面识别承载重要业务与服务的网络资产，编制资产清单，动态维护资产之间的关联和依赖关系。金融机构应按重要程度对资产进行分类分级管理，明确资产管理

责任部门及责任人，集中统一管理网络资产。

第十七条 【网络安全域】

金融机构应当结合业务与数据重要程度、所面临网络安全威胁程度以及遭遇网络攻击后所受影响的范围等情况，划分不同功能、等级的网络安全域，明确不同安全域的隔离方式和防护要求，有效隔离内外部网络以及总部、境内外分支和附属机构之间网络。

第十八条 【访问控制策略】

金融机构应当集中管理网络安全边界，统一制定网络安全规则和监测标准，按照“最小必要”原则配置网络访问控制策略，严格控制跨域访问。

第十九条 【互联网边界防护】

金融机构应当重点实施生产网和互联网之间的边界防护，统一管理互联网出口，建立网络攻击监测与防御体系，综合运用访问控制、入侵防御、抗拒绝服务攻击等网络边界安全防护和数据保护措施，有效抵御网络入侵攻击行为。

第二十条 【内部网络边界防护】

金融机构应重点防护承载重要信息系统、敏感级及以上数据的内部网络边界，采取必要的技术手段，及时识别并阻断各类网络攻击行为与数据泄露风险。

第二十一条 【安全基线】

金融机构应当建立网络安全配置策略，明确操作系统、网络设备、中间件、数据库、应用软件等网络资源的安全基

线，定期核查基线配置有效性。

第二十二条　【日志记录】

金融机构应当开展网络安全相关日志管理，日志管理应当满足法律法规和监管要求，以及网络安全监测预警、事件分析处置工作需要，日志留存期限不少于六个月。

第二十三条　【漏洞缺陷管理】

金融机构应当开展网络安全漏洞缺陷管理，建立分级处置和闭环管理机制，定期开展安全漏洞扫描，有效识别漏洞缺陷并及时处置，无法按时完成处置的应当采取风险缓释措施。每季度至少开展一次漏洞缺陷处置情况分析。发现可能对行业造成影响的漏洞缺陷，应当立即向国家金融监督管理总局或者其派出机构报告。

第二十四条　【应用软件安全】

金融机构通过互联网应用程序提供服务的，应用程序应当符合相关国家要求。金融机构发现应用程序存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第二十五条　【开发测试管理】

金融机构应加强开发项目全生命周期管理，建立软件开发测试安全规范和管控流程，综合采取安全方案评审、源代码安全检查、组件风险排查、安全测试等措施提高软件开发质量。对应用产品业务逻辑安全开展评估测试，防范非授权访问等缺陷。

第二十六条　【变更安全管理】

金融机构开展可能影响网络安全的投产变更，应当充分评估技术和业务风险，制定风险防控、应急处置和系统回退方案，并对投产变更结果进行复核验证。金融机构的互联网信息系统、等保三级及以上网络和重要信息系统，投产或重大变更前应当通过安全测试评估。原则上不得在业务高峰期和敏感时段实施重大投产变更。

第二十七条　【角色访问控制】

金融机构应当建立用户认证和访问控制管理流程，根据网络区域、系统和数据的重要性和敏感程度，按照“最小必要”原则分配访问权限，对用户角色进行唯一身份标识与鉴别，定期开展权限审计，及时清理不当权限。

第二十八条　【远程访问权限】

金融机构应当规范网络远程接入安全管理，采用多因素认证、白名单等方式控制远程网络接入，限定访问时段、操作范围和权限等级，使用结束后及时回收所有权限，定期核查远程访问权限使用情况。

第二十九条　【终端介质管控】

金融机构应将终端安全纳入统一管控，开展终端软件缺陷管理，及时监控并阻断非法存储介质使用等违规行为，定期开展安全检查。终端和存储介质报废或重用前应当进行有效的数据清除，防止数据泄露。

第三十条　【供应链安全】

金融机构应当建立信息科技供应链安全风险管理制度，选用符合国家有关规定的信息技术产品及服务，建立供应链产品清单，主动识别供应链安全风险。与提供重要外包服务的供应商签订服务水平协议，制定供应中断应急预案并开展演练。发现可能对行业造成影响的供应链安全风险，应当及时向国家金融监督管理总局或者其派出机构报告。

第三十一条　【新技术安全】

金融机构应当建立新技术应用安全评估机制，新技术引入前应当开展安全评估，不得因引入新技术而降低网络安全防护水平。

第三十二条　【外包安全管理】

金融机构应当按照信息科技外包监管要求，开展外包准入、服务提供商管理、外包人员管理、外包风险评估检查等相关工作。

第三十三条　【网络安全等级保护】

金融机构应当落实国家网络安全等级保护制度要求，履行网络安全等级保护义务，依据法律法规和监管要求开展网络安全等级保护定级备案、测评整改等工作，三级及以上网络每年至少开展一次等级测评。

第三十四条　【密码安全管理】

金融机构应当落实国家商用密码管理制度要求，开展密码保障系统的规划、建设、运行和商用密码应用安全性评估等工作，使用符合国家相关要求的密码产品和服务。

第三十五条　【数据安全管理】

金融机构应当按照法律法规和监管要求履行数据安全保护义务，建立健全数据安全管理制度，明确数据安全主体责任及牵头部门，开展数据分类分级，构建覆盖数据处理活动和应用场景的安全保护机制，规范数据处理活动，依法合规使用数据。

第三十六条　【个人信息安全管理】

金融机构应当按照法律法规和监管要求履行个人信息保护义务，采取技术和管理措施对个人信息进行保护。鼓励金融机构接入国家网络身份认证公共服务，开展用户真实身份核验、认证。

第四章　网络安全风险监测

第三十七条　【网络安全监测预警机制】

金融机构应当建立健全网络安全风险监测预警机制，构建多层级多渠道监测防护体系，优化监测指标，及时评估监测预警信息，按要求向国家金融监督管理总局或者其派出机构报告。金融机构应当加强对网络安全威胁形势的跟踪分析，充分识别可能对本机构造成重大影响的网络安全风险，及时优化调整监测、预警体系，并采取必要的防护措施。

第三十八条　【网络安全风险监测与分析】

金融机构应实时监测网络和信息系统运行状态，综合分析流量数据、日志数据、告警信息、安全事件信息，及时预

警网络攻击、系统异常访问、异常网络流量以及人员异常操作，主动监测钓鱼网站、仿冒客户端软件、仿冒官方媒体账号等威胁。

第三十九条　【威胁情报共享和服务合作】

金融机构应当开展网络安全威胁情报共享和合作，多渠道获取威胁情报信息，及时分析研判金融管理、网信、公安等部门通报的网络安全风险。涉及其他金融机构或可能对行业造成影响的威胁情报，应立即通过网络安全态势感知监管平台向国家金融监督管理总局或者其派出机构报告。

第四十条　【网络安全风险闭环管理】

金融机构应当充分运用网络流量、系统运行状态和网络安全威胁情报等信息，开展网络攻击、资产风险、异常行为和安全事件分析，综合研判本机构网络安全风险状况，并根据风险严重和紧急程度及时处置或者采取风险缓释措施，消除风险隐患或降低风险影响。

第四十一条　【网络安全风险评估和审计】

金融机构应当每年至少开展一次网络安全风险评估和互联网渗透测试，评估范围应当覆盖本机构、境内外分支机构和附属机构。每三年至少开展一次网络安全审计。

第五章　网络安全事件响应与处置

第四十二条　【网络安全事件分级】

金融机构应当建立网络安全事件管理制度，依据银行业

保险业网络安全事件分级标准（详见附件）细化制定本单位网络安全事件分级规则。

第四十三条　【网络安全应急响应与处置机制】

金融机构应当建立网络安全事件应急响应与处置组织架构，确定应急决策层、指挥层、执行层、保障层等的人员构成，明确职责分工，规范工作流程，建立协调机制，落实资源保障。应急决策层应当由高级管理人员组成，负责决策网络安全事件应急处置中的重大事项。

第四十四条　【应急预案和演练】

金融机构应当按照国家网络安全事件应急预案框架和监管要求，制定覆盖各类网络安全突发事件场景的应急预案，明确预案启动条件、应急处理流程、系统恢复步骤等内容，定期更新应急预案，每年至少组织开展一次应急演练，将提供重要外包服务的供应商纳入演练范围。

第四十五条　【事件报告】

金融机构应当建立网络安全事件报告制度，明确网络安全事件报告流程、渠道、时限等要求，报告内容应当至少包括时间、地点、网络和系统名称、事件过程、处置进展、事件影响等。

发生较大（三级）及以上的网络安全事件，金融机构应当于 2 小时内向国家金融监督管理总局或者其派出机构报告，并在事件发生后 24 小时内提交正式书面报告。其中，发生特别重大（一级）网络安全事件，金融机构应当立即采

取处置措施，按照规定及时告知用户并向国家金融监督管理总局或者其派出机构报告,每 2 小时报告处置进展，直至处置结束。

第四十六条　【事件响应处置】

金融机构发生网络安全事件后，应立即启动应急预案，对网络安全事件进行调查、评估和处置，采取技术措施和其他必要措施，有效降低网络安全事件影响，防止危害扩大。及时向社会发布与公众有关的警示信息，对公安机关依法维护国家安全和侦查犯罪的活动提供必要的协助。

第四十七条　【系统和数据恢复】

金融机构发生网络安全事件后，应当充分识别网络安全事件对业务系统和数据的影响，按照应急预案及时恢复受影响的业务系统，对相关业务数据进行核对，追补丢失数据，并对恢复结果进行验证，确保业务系统正常运行。

第四十八条　【分析与改进】

金融机构应当在事件处置完成后，总结分析事件成因、影响程度和处置过程，识别网络安全防护体系以及应急预案存在的问题缺陷，并整改完善。较大（三级）及以上网络安全事件应急处置结束后五个工作日内，应当向国家金融监督管理总局或者其派出机构报送事件处置总结报告。

第四十九条　【审计与评估】

金融机构发生重大（二级）及以上网络安全事件后，应当及时开展专项审计，查实问题根源，督促问题整改到位。

金融机构应当定期评估网络安全风险及事件处置情况，识别并整改网络安全防护体系以及应急预案存在的问题，确保风险管理措施和应急处置机制持续有效。

第五十条 【责任追究】

对因管理不当造成较大（三级）及以上网络安全事件，或者瞒报、漏报、谎报、故意迟报较大（三级）及以上网络安全事件的，金融机构应当严肃追责问责。

第六章 关键信息基础设施管理

第五十一条 【关基认定、变更】

金融机构应当按照金融业关基认定规则要求，配合开展本机构关基认定工作。

关基运营者应当建立维护关基资产清单，关基发生较大变化、可能影响关基认定结果的，应当及时向国家金融监督管理总局报告。

第五十二条 【关基防护总体要求】

关基运营者应当采取保护措施，确保关基安全稳定运行，维护数据完整性、保密性和可用性。关基运营者主要负责人对关基安全保护负总责。

关基运营者应当落实关基商用密码管理规定、网络安全等级保护制度，开展商用密码应用安全性评估。关基网络安全保护等级不低于第三级。

第五十三条 【关基安全保护框架】

关基运营者应当明确关基保护目标，制定关基安全保护方案，按年度制定关基安全保护计划并组织实施，及时报送重大网络安全事件及威胁。

第五十四条　【明确安全管理部门】

关基运营者应当明确关基安全管理部门，制定保护制度和计划，建立安全专业队伍，认定关键岗位。组织实施对关基活动的安全保护，开展安全监测和风险评估。安全管理部门负责人及关键岗位人员应进行安全背景审查。

第五十五条　【关基建设管理】

关基保护措施应当与关基规划、建设、使用同步开展，确保安全保护措施有效。关基运营者应当具备关基系统自主研发能力，关键技术应自主掌握。

第五十六条　【关基产品和服务安全管理】

关基运营者采购网络产品和服务时，应与提供者签订安全保密协议并监督其执行。可能影响国家安全的，应当通过国家网络安全审查。关基运营者应当优先采购安全可信的网络产品和服务。关基运营者应当向国家金融监督管理总局报送年度网络产品和服务、云计算服务采购清单。

第五十七条　【关基安全运行要求】

关基应当在中国境内运行维护，定期实施漏洞扫描、容量评估，及时处置风险。关基同城和异地灾备中心应具备完全接管生产和长期运行的能力，每年开展面向高风险场景的真实演练。

第五十八条　【关基技术保障体系】

关基运营者应当建立网络纵深防御体系，监测异常行为、拦截恶意程序、阻断未授权访问。关基管理后台应采取双因素认证和白名单访问措施。

第五十九条　【关基安全运营要求】

关基运营者应当建立 7×24 小时运营的网络安全监控指挥中心，实时监测风险，开展态势分析和预警，组织应急处置。

第六十条　【关基应急预案和演练】

关基运营者应当制定关基网络安全事件应急预案，至少包括关键功能、应急场景、恢复时间、应急流程等，每年开展安全攻防演练，履行报批备案程序。

第六十一条　【关基安全事件管理】

关基发生较大（三级）及以上网络安全事件，关基运营者应当第一时间向国家金融监督管理总局、公安部门报告，最迟不得超过 1 小时。事件恢复后立即开展专项审计并及时整改。

第六十二条　【关基供应链安全】

关基运营者应当加强供应链安全管理，维护关基供应商目录，加强监测、及时处置风险。关基外包服务应纳入重要外包管理。

第六十三条　【关基风险评估】

关基运营者应当每年开展关基网络安全检测和风险评估，内容包括等保测评、商密评估、国家标准落实、数据安全和个人信息保护、网络安全事件监测及处置等，及时整改问题。

第七章　监督管理

第六十四条　【监督管理职责】

国家金融监督管理总局及其派出机构依法履行以下监督管理职责:

（一）组织银行业保险业落实国家关于网络安全的法律法规、方针、政策和重大部署;

（二）组织制定并推动落实银行业保险业网络安全监管制度;

（三）组织对金融机构开展网络安全非现场监管和现场检查;

（四）负责金融机构网络安全风险监测预警和信息通报、关键信息基础设施监督管理、网络安全事件调查处置等工作;

（五）与网信、公安等国家网络安全主管部门建立联防联控管理机制;

（六）根据有关法律法规采取监管措施或者实施行政处罚;

（七）法律法规规定的其他网络安全监管职责。

第六十五条　【监管报告】

金融机构应当将网络安全年度工作情况纳入信息科技年度工作报告，每年1月15日前向国家金融监督管理总局或其派出机构报送。报告内容应当包括网络安全治理、网络安全建设和运行管理、网络安全风险监测、事件响应与处置、关基安全保护年度计划和年度工作总结、关基检测评估和整改情况等。

第六十六条　【监督检查】

国家金融监督管理总局及其派出机构通过监管评级、风险提示、监管通报、监管会谈等非现场监管和现场检查方式，实施对金融机构网络安全管理的持续监管。可以通过网络攻防演练、互联网渗透测试等方式对金融机构实施网络安全测试，可以委托有关专业机构对金融机构开展网络安全检查。

第六十七条　【监管处罚】

金融机构违反本办法有关规定的，国家金融监督管理总局及其派出机构应当责令改正，并根据其违规情况依法采取监管措施，情节严重的依法实施行政处罚。

第六十八条　【行业自律】

中国银行业协会、中国保险行业协会等行业自律组织可以依法制定行业网络安全自律规则，通过宣传、培训、协调、服务等方式，引导金融机构提高网络安全管理水平，提升网络安全风险防范能力。

第八章　附　则

第六十九条　【术语定义】

本办法下列术语定义:

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）重要信息系统，是指支撑重要业务，其信息安全和系统服务安全关系公民、法人和组织的权益或者社会秩序和公共利益，甚至影响国家安全的信息系统。包括但不限于面向客户、涉及账务处理、时效性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统，支撑上述系统运行的机房和网络等基础设施也应当作为重要信息系统的一部分。

（四）关键信息基础设施，简称关基，是指一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的金融机构重要网络设施、信息系统等。

第七十条　【另有规定】

国家对处理、存储涉及国家秘密和工作秘密信息的网络安全管理另有规定的，从其规定。

国家法律、行政法规、其他中央金融管理部门以及网信、公安、工信、保密和密码等部门对金融机构网络安全工作做出规定的，金融机构应当遵照执行。

第七十一条　【解释和修订】

本办法由国家金融监督管理总局负责解释、修订。

第七十二条　【生效日期】

本办法自颁布之日起施行。

附件

银行业保险业网络安全事件分级标准

网络安全事件依照其影响范围及持续时间、系统重要程度、资金损失以及对国家安全、社会秩序、经济建设和公众利益造成的影响等因素分为四级，当同时满足多个级别的定级条件时，按更高级别确定事件等级。

（一）特别重大（一级）网络安全事件:

1. 网络安全原因导致敏感级及以上数据遭到泄露、破坏、非法获取、非法利用，构成特别重大数据安全事件;

2. 网络安全原因导致重要信息系统服务异常，在业务服务时段导致金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达 3 个小时（含）以上，或者一个省（自治区、直辖市）业务无法正常开展达 6 个小时（含）以上的网络安全事件;

3. 符合下列情形之一，对国家安全、社会秩序、经济建设、公众利益构成特别严重威胁、造成特别严重影响、产生特别重大经济损失的网络安全事件:

（1）互联网网站、移动互联网应用系统等重要信息系统被攻击篡改导致违法有害信息大范围传播;

（2）关键信息基础设施被入侵并获取系统管理权限;

（3）网络安全原因导致重要信息系统服务中断;

（4）网络安全原因导致的其他事件。

（二）重大（二级）网络安全事件:

1.重要数据、敏感数据遭到泄露、破坏、非法获取、非法利用，构成重大数据安全事件;

2.网络安全原因导致重要信息系统服务异常，在业务服务时段导致金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达半个小时（含）以上、3个小时以下，或者一个省（自治区、直辖市）业务无法正常开展达3个小时（含）以上、6个小时以下的网络安全事件;

3.符合下列情形之一且未达到特别重大事件级别的，对国家安全、社会秩序、经济建设、公众利益构成严重威胁、造成严重影响、产生重大经济损失的网络安全事件:

（1）互联网网站、移动互联网应用系统等重要信息系统被攻击篡改导致违法有害信息较大范围传播;

（2）关键信息基础设施外其他重要信息系统被入侵并获取系统管理权限;

（3）网络安全原因导致重要信息系统服务中断;

（4）网络安全原因导致的其他事件。

（三）较大（三级）网络安全事件:

1.重要数据、敏感数据遭到泄露、破坏或者非法获取、非法利用构成较大数据安全事件;

2.网络安全原因导致重要信息系统服务异常，在业务服务时段导致一个省（自治区、直辖市）业务无法正常开展达

半个小时（含）以上、3 个小时以下的网络安全事件;

3. 符合下列情形之一且未达到重大及以上事件级别的，对国家安全、社会秩序、经济建设、公众利益构成较严重威胁、造成较严重影响、产生较大经济损失的网络安全事件;

（1）互联网网站、移动互联网应用系统等重要信息系统被攻击篡改并造成影响;

（2）重要信息系统被入侵，其他信息系统被入侵并获取系统管理权限;

（3）网络安全原因导致重要信息系统服务中断;

（4）网络安全原因导致的其他事件。

（四）一般（四级）网络安全事件

除上述网络安全事件外，对组织或者个人造成一定影响的网络安全事件，或者因网络安全原因导致的一般数据安全事件。