网上基金销售信息系统技术指引

第一章 总则

第一条 为保障网上基金销售信息系统的安全、可靠、高效运行，促进基金销售业务健康有序发展，保护投资者的合法权益，依据《中华人民共和国证券投资基金法》《公开募集证券投资基金销售机构监督管理办法》《证券期货业网络和信息安全管理办法》《证券基金经营机构信息技术管理办法》《证券期货业网络安全事件报告与调查处理办法》等法律法规，制定本指引。

第二条 按照《公开募集证券投资基金销售机构监督管理办法》从事基金销售业务的机构，开展网上基金销售业务，适用本指引。

本指引所称网上基金销售是指利用互联网、移动互联网等技术手段为投资者开立基金交易账户，宣传推介基金，办理基金份额发售、申购、赎回及提供基金交易账户信息查询等活动。

第三条 网上基金销售信息系统是指基金销售机构在网上开展基金销售业务活动中所采用的网络设备、计算机设备、软件及专用通信线路等构成的信息系统，包括门户网站、网上基金销售系统投资者端和服务端。

第四条 基金销售机构应当平衡发展与安全，采取相应的技术和管理措施，落实国家政策法规及监管部门要求，提

升信息科技应用水平，夯实网络和信息安全保障能力，保证网上基金销售系统连续性、合规性及安全性，并做好系统信息保密工作。

第五条 基金销售机构从事网上基金销售，应当遵守法律法规、中国证券监督管理委员会（以下简称中国证监会）规定和中国证券投资基金业协会（以下简称协会）自律规则。协会对基金销售机构执行本指引的情况进行指导和督促。

第二章 基本要求

第六条 基金销售机构应当对网上基金销售信息系统统一规划、集中管理，为子公司提供网上基金销售信息系统服务，应当按照中国证监会有关规定签署服务协议，明确各方义务职责，加强共用基础设施安全防范。

服务协议包含但不限于服务范围、服务方式、服务期限、职责义务、业务功能、技术指标、知识产权、保密要求、违约责任、争议与仲裁等。

第七条 基金销售机构应当按相关法律法规和政策标准要求，结合自身综合情况，制定网上基金销售信息系统相关管理制度，包含但不限于管理组织、人员配备、系统建设、运行管理、应急措施、风险处置、容灾备份、系统安全、数据安全、系统审计、技能培训等。

第八条 基金销售机构应当将网上基金销售信息系统的风险管理纳入本机构风险控制工作范围，建立健全网上基金销售风险控制管理体系。基金销售机构结合年度风险管理评

估总体安排，每年至少开展一次网上基金销售信息系统风险管理有效性评估。风险评估可以参考《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022），必要时可聘请外部专业机构协助开展评估工作。

第九条 网上基金销售信息系统应当部署在中华人民共和国境内，满足监管部门现场检查要求及司法机关调查取证要求。

第十条 基金销售机构应当采用适当方式与投资者签订网上基金业务服务协议或合同，明确双方的权利、义务和风险的责任承担，向投资者揭示使用网上基金销售信息系统可能面临的风险、基金销售机构已采取的风险控制措施和投资者应当采取的风险防范措施。

第十一条 基金销售机构应当妥善保存网上基金销售过程形成的电子合同、风险揭示书、风险调查问卷等电子材料，保存期限、保存形式应当符合法律法规、自律规则的要求，满足投资者及相关当事人查阅、下载等需求，满足监管部门、司法机关现场检查及调查取证等要求。

第十二条 网上基金销售信息系统应当具备账户管理、基金交易、信息查询、投资者服务及对管理者操作行为审计功能；应当具有向投资者提示交易时间区间的功能，交易时间区间应当严格遵守监管部门或交易所的相关规定。

第十三条 基金销售机构应当建立可靠的运行环境，科学合理设定基金销售信息系统处理能力、存储容量和通讯带宽等非功能指标，加强信息系统吞吐量、用户并发量等信息

系统性能监控，及时发现潜在风险，满足业务增长的实际需要。

基金销售机构可以适时引入动态资源管理机制，增强资源自动扩展或缩减，保障网上基金销售信息系统访问高峰期稳定运行、及时响应，提高信息系统运营效率。

第十四条 基金销售机构应当通过自身运营管理的信息系统直接接收投资者交易指令，并记录投资者交易指令接收时间，但法律法规及中国证监会另有规定除外。

第十五条 网上基金销售信息系统重大版本上线或升级，应当开展技术论证和上线验证，对上线实施行为进行审查与跟踪。

网上基金销售信息系统不得在基金交易时段（一般为工作日 9 时至 15 时）对生产环境进行变更，但因存在重大故障缺陷，可能有损投资者合法权益，对资本市场正常交易产生不良影响，经评估必须进行紧急修复的情况除外。

第十六条 网上基金销售信息系统因功能升级等情况，相关服务需要暂停或暂时下线，经评估将影响正常展业时，基金销售机构应当做好系统替代等安排，并通过门户网站公告、系统通知、短信通知等方式，提前 3 日告知投资者。

第十七条 基金销售机构计划彻底停用网上基金销售信息系统，应当组织开展相关影响评估，妥善制定信息系统停用方案，提供备用业务办理方式，通过官方有效渠道向投资者进行公告提示，保障投资者合法权益。涉及移动互联网应用程序停用的，还应符合相关规定。

第十八条 基金销售机构应当结合实际情况，参考《证券期货经营机构信息系统备份能力标准》(JR/T 0059-2010)，科学规划网上基金销售信息系统数据备份能力、故障应对能力、灾难应对能力和重大灾难应对能力，合理设定数据备份频率、数据验证频率、数据备份存放介质、系统恢复时间目标、系统恢复点目标等关键要素，确保投资者网上基金交易业务连续性和数据完整性。

网上基金销售信息系统应当接入2个以上不同运营商互联网线路，采取有效的负载均衡技术，避免在同一运营商互联网线路方面出现单点故障和带宽瓶颈。

第十九条 基金销售机构应当结合发展战略、市场交易规模等因素，每年至少开展一次网上基金销售信息系统压力测试和评估分析，包含但不限于用户并发在线数、服务端存储空间、数据表空间容量、业务响应时间、应用系统交易处理性能等，确保各项指标满足业务发展需要。

第二十条 基金销售机构委托或借助信息系统技术服务机构研发运维网上基金销售信息系统，应当与其签订商业合同及保密协议，并确保信息系统运行始终处于自身控制范围。

基金销售机构应当要求信息系统技术服务机构提供的产品具备合法知识产权，源代码通过漏洞安全审查。明确信息系统技术服务机构在未取得基金销售机构许可的情况下，不得截取、存储、转发和使用基金业务活动相关经营数据和投资者数据等。

基金销售机构应当定期组织对信息系统技术服务机构

提供的产品和服务连续性进行评估，确保满足业务发展需要和投资者利益，不因委托关系而免除或减轻其依法应当承担的责任。

第二十一条 基金销售机构应当落实网络安全等级保护制度，依法履行网络安全等级保护义务，按照监管部门有关指导意见，对网上基金销售信息系统及时开展定级备案工作。

第二十二条 基金销售机构应当落实密码相关规定要求，加强密码技术应用，保障网上基金销售信息系统的真实性、机密性、完整性和不可否认性。网上基金销售信息系统采用的密码技术、服务、产品应当符合国家密码管理政策和标准规范。

第二十三条 基金销售机构应当加强网上基金销售信息系统全面支持互联网协议第六版（以下简称 IPv6）能力，建立健全 IPv6 监控运维体系。

第三章 门户网站

第二十四条 门户网站是指基金销售机构建设的具备开户交易或客户资料修改、信息发布、业务咨询、营销推广、投资者服务和投资者教育等功能的网站。

第二十五条 门户网站应向当地电信主管部门申请互联网信息服务（以下简称 ICP）备案，根据网络系统安全管理

的相关要求向公安机关备案，并于网站首页公布 ICP 备案号和网安备案号，为投资者提供查询门户网站备案信息链接。

第二十六条 门户网站不得存放与基金交易业务有关的投资者、基金交易和账户口令等敏感数据。

第二十七条 基金销售机构应当建立对门户网站内容发布的审核、管理和监控机制，提升对页面内容的实时监测能力，对有害信息进行过滤，杜绝因其内容不合法、不真实、不准确等造成不良影响。

第二十八条 门户网站应当建立链接地址的监测巡检机制，确保所有链接有效可用，及时清除不可访问的链接地址，避免产生“错链”、“断链”。

第二十九条 门户网站应当建立安全监测预警机制，实时监测网站的应用系统、网站数据等运行状态以及网站挂马、内容篡改等攻击情况，及时对异常情况进行报警和处置。

第三十条 门户网站应当采用服务器电子证书等技术手段，加强门户网站可信度和有效识别。基金销售机构应当将防范假冒钓鱼网站场景纳入网络和信息安全宣传范畴。

第四章 网上基金销售信息系统投资者端

第三十一条 网上基金销售信息系统投资者端是指基金销售机构提供的，由投资者通过互联网、移动互联网等非现场方式独自完成业务操作的应用系统，包含网页交易程序、桌面应用程序、移动互联网应用程序等。

第三十二条 网上基金销售信息系统投资者端应当具备如下功能：

（一）向投资者提示异地登录或者非常用设备登录信息。同时，提供登录网络协议地址（IP）所属地区、日期及时间等信息查询功能；

（二）在指定的闲置时间间隔到期后，自动锁定投资者端的使用或退出；

（三）履行法律法规赋予投资者在个人信息保护方面的各项权利的义务，并向投资者展示隐私政策；

（四）在投资者购入基金前，应当提示投资者阅读与基金产品相关的重要信息，重点关注产品费率等信息，提供有效途径供投资者查询，并以显著、清晰的方式向投资者揭示投资风险；

（五）根据投资者合理要求，提供相关基金产品信息、交易对账信息等查询服务；

（六）根据投资者意愿设置禁扰名单与禁扰期限，明确内部追责措施，防止因营销活动对投资者产生信息骚扰；

（七）履行法律法规、自律规则规定的基金销售程序，落实相应的基金销售要求。

第三十三条 基金销售机构通过网上基金销售信息系统受理投资者开立基金交易账户申请时，应当要求基金投资者提供身份证明信息，采取等效实名制方式核实投资者身份，为投资者开立基金交易账号，并开通相应的信息查询、交易操作、交易限额、资金划转等功能。

第三十四条 网上基金销售信息系统应当具备可靠的身份验证机制，确认投资者身份有效性和合法性，避免不法分子利用黑客程序窃取投资者账号和口令。

涉及投资者首次登录和基金交易等重要业务场景，网上基金销售信息系统应当采用双因素认证模式，加强投资者身份鉴别。

第三十五条 网上基金销售信息系统不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或者变相强迫投资者同意收集、使用和基金销售业务无直接关系的信息。

网上基金销售信息系统收集、使用个人生物特征、个人行踪等敏感信息，应当以明确的方式逐项取得投资者同意。

第三十六条 网上基金销售信息系统投资者端不得在投资者本地计算机储存投资者口令等重要信息；为便于投资者使用而储存账户信息的，应在投资者选择同意的情况下进行储存；确需存储其它信息的，投资者本地存储数据仅为参考数据，应当以基金销售机构记录数据为最终准确数据。

第三十七条 网上基金销售信息系统投资者端应当具有投资者账户口令复杂度控制和口令定期修改提醒机制；自动初始口令必须采取最小有效期限或强制首次登录修改要求。自动初始口令禁止生成相同口令或弱口令。

网上基金销售信息系统投资者端应当具备口令修改和取回操作日志记录的功能。

第三十八条 网上基金销售信息系统投资者端与基金销售支付结算等基金销售服务机构信息系统进行数据通信，应

当使用数字加密技术，确保数据信息的发送和接收始终处于受到保护状态。

第三十九条 投资者访问网上基金销售信息系统时，未经投资者许可，除提高程序安全性和稳定性的必要控件以外，不得以任何方式在投资者信息系统安装插件。

第四十条 基金销售机构借助应用程序接口模式向投资者提供网上基金交易服务的，应当要求投资者登记交易终端信息，加强交易终端合法身份认证；信息发生变更的，应当要求投资者履行变更程序，确保投资者所使用的交易终端信息与登记内容一致。

基金销售机构应当加强应用程序接口版本规划与管理，确保新旧应用程序接口的兼容性、适配性和可扩展性，保证网上基金销售信息系统服务业务连续性。

第四十一条 基金销售机构应当规范面向投资者使用的移动互联网应用程序开发及运营，委托第三方检测认证机构、行业测试中心等专业机构开展安全认证，确保程序开发、个人信息处理、数据安全、密码应用、安全管理等方面符合国家及行业标准要求。

第五章 网上基金销售信息系统服务端

第四十二条 网上基金销售信息系统服务端是指基金销售机构通过互联网向投资者提供网上基金交易、基金账户信息查询等服务的信息系统，包括互联网接入、安全防护与监控、应用服务、身份认证等相关子系统。

第四十三条 网上基金销售信息系统服务端应当具备向投资者提供查询预留验证信息功能服务，帮助投资者识别仿冒的网上基金销售信息系统，防止不法分子利用仿冒的网上基金销售信息系统进行诈骗活动或盗取账号口令等信息。

第四十四条 网上基金销售信息系统服务端应当保障对投资者的授权不被恶意提升或转授，防止投资者访问未经过授权的数据，使用未经授权的功能。

第四十五条 基金销售机构开展网上基金销售业务，需要对投资者信息和交易信息等使用电子签名或电子认证时，应当遵照国家有关法律法规的规定。

网上基金销售信息系统服务端采用认证授权和加密体系应当具备足够的强度和抗攻击能力，并根据网上基金销售业务的安全性需要和信息科技的发展，定期检查，适时调整。

第四十六条 网上基金销售信息系统服务端与基金销售机构及投资者以外的第三方进行数据交换，应当经过认证后仅向指定地址发送信息。未经基金销售机构授权，不得与基金销售机构及投资者以外的第三方进行任何形式的数据交换。

第四十七条 网上基金销售信息系统服务端应当能够抵御连续猜测，防止攻击者通过对合法账户进行大规模非法登录请求，导致大量用户账户被异常锁定而正常无法登录。

第四十八条 网上基金销售信息系统服务端对数据包被篡改、异常重发等情况需具有应对能力。

第四十九条 网上基金销售信息系统服务端应当能在指定的闲置操作时间限制到期后，自动终止服务请求访问。

第五十条 网上基金销售信息系统服务端应当记录并存储能识别服务请求方身份的内容、业务操作、文件下载等日志信息，确保数据的可审计性，满足监管部门、行业协会现场检查要求及司法机关调查取证的要求。

第五十一条 网上基金销售信息系统服务端应当能够有效屏蔽系统技术错误信息，避免将信息系统产生的错误信息直接反馈至投资者端，防止泄露投资者相关信息。

第五十二条 网上基金销售信息系统服务端应当能够提供系统运行状况信息(如活动状态、并发在线数目、并发会话数目、线程数目、队列长度等)、错误信息、安全警告等。

第五十三条 网上基金销售信息系统服务端应当定期开展维护和升级，内容包括但不限于软件更新、硬件检查、网络服务端口核查和性能优化等，确保信息系统的稳定性和安全性。因维护和升级操作，可能影响投资者正常使用的，基金销售机构应当通过适当途径提前告知投资者。

第五十四条 网上基金销售信息系统服务端应具备防范结构化查询语言（SQL）注入、跨站脚本、会话（Session）欺骗、拒绝式服务攻击和缓冲区溢出等各类互联网入侵攻击的能力。

第六章 安全管理

第五十五条 网上基金销售信息系统应当明确安全责任人，落实安全保护责任。加强网络和信息安全培训，定期对机构全员及相关人员进行不同层次的安全教育、技术培训和技能考核，增强网络和信息安全防范意识，提高网络和信息安全防护水平。

第五十六条 网上基金销售信息系统的开发测试环境与生产环境应当有所分离。服务于网上基金销售信息系统开发、测试及运维人员应当有所分离；未经授权，开发、测试人员不得访问或修改网上基金销售信息系统生产环境。

第五十七条 基金销售机构应当对网上基金销售信息系统各个子系统合理划分安全域，对不同安全域之间采用物理或逻辑隔离，防止恶意攻击和非法访问，防范安全风险跨域传导。

第五十八条 基金销售机构应当合理规划账号体系，严格管理网上基金销售信息系统相关网络安全设备、服务器、数据库、中间件及应用系统等账号；清除所有冗余和无关账号；按最小权限原则设置账号权限；避免使用最高权限账号执行一般性操作。

第五十九条 网上基金销售信息系统各级管理账号和口令应当由专人负责，口令长度应为 12 位以上，混有字母、数字和特殊字符，区分大小写，并定期更改。

基金销售机构应当每季度至少开展一次网上基金销售系统账户权限使用情况及口令更改情况审查评估，并形成评估报告。

第六十条 基金销售机构应当妥善保存网上基金销售信息系统的技术文档、用户手册及培训材料等，技术文档应当包含但不限于规划、设计、开发、测试、上线、变更及运维过程中产生的各类文档，并定期开展文档日志检查，确保文档材料的有效性。

第六十一条 基金销售机构应当健全网上基金销售信息系统配置管理制度，加强对配置的版本控制，确保所涉及的软硬件环境配置信息的完整性和可跟踪性。基金销售机构应当定期对配置信息开展有效性确认。

第六十二条 基金销售机构应当及时对应用于网上基金销售信息系统的相关服务器、存储设备、网络设备、安全设备及操作系统、数据库、应用软件进行版本升级或漏洞补丁。升级实施前，应当制定稳妥的技术方案，开展风险评估和全流程测试，确保基础资源的连续可用性。

第六十三条 网上基金销售信息系统应当严格保护投资者、基金交易、账号口令等敏感信息，并以密文形式存储上述信息。

基金销售机构利用互联网、移动互联网传输投资者、基金交易、账号口令等敏感信息，应当采用加密传输等技术手段，传输过程非必要不得对信息进行解密处理，确保数据的保密性、完整性、真实性。

第六十四条 网上基金销售信息系统应部署防火墙、入侵检测系统或入侵防护系统，定期开展漏洞扫描、渗透测试等安全检测及安全日志检查，提高网上基金销售信息系统的防护能力。

基金销售机构应当确保网上基金销售信息系统服务器采取技术手段防止恶意代码（病毒等）运行、传播；及时更新病毒库，定期对网上基金销售信息系统开展全面的病毒扫描。

第六十五条 基金销售机构应当采取有效措施对门户网站上提供的网上基金投资者端应用程序进行保护，对投资者端应用程序进行严格的病毒扫描和木马检查，并通过专用安全手段传输至相关文件下载服务器。

第六十六条 基金销售机构应当对网上基金销售信息系统运行状况进行实时监控，建立异常事件的甄别、报警、处理和报告机制。

基金销售机构应当全面、准确记录并妥善保存网上基金销售信息系统运行监测日志，日志应当保存六个月以上。运行监控范围应当包括服务器、存储设备、网络设备、安全设备及操作系统、数据库、应用软件、通讯线路状态等。

基金销售机构应当每季度至少开展一次监控信息评估分析，形成报告并存档。

第六十七条 基金销售机构应当建立应急处置组织体系，对电力、通信等基础设施、计算机硬件或网络设备、操作系统或应用系统等可能的故障及病毒入侵、恶意攻击、误操作、不可抗力等情况，制定应急方案。

基金销售机构应当根据最新安全发展态势需要，每年至少开展一次应急演练及应急预案评估，结合外部要求和业务发展变化对应急预案进行及时修订，确保所有相关人员熟悉应急流程和操作。

第六十八条 网上基金销售信息系统发生技术故障，影响正常展业，基金销售机构应当立即启动应急预案，尽快恢复信息系统运行，保障相关业务连续性。根据《证券期货业网络安全事件报告与调查处理办法》要求，及时向监管部门报告，并抄报协会。

第七章 附则

第六十九条 本指引下列用语含义如下：

（一）本指引中所称应用程序接口，是指除网页交易程序、移动互联网应用程序等标准化交易系统外，基金销售机构向具有个性化需求并且符合规定条件的特定投资者提供接口服务；

（二）本指引中所称敏感数据是指如果被损毁、泄露可能对证券期货市场或投资者合法权益造成严重影响的数据，包括但不限于投资者信息、基金交易数据、账户口令信息等；

（三）“以上”包括本数，“以下”不包括本数。

第七十条 【发布实施】本指引自2025年1月1日起施行。《网上基金销售信息系统技术指引》（中基协发〔2012〕13号）同时废止。