中国证券业协会关于发布《网上基金销售信息系统技术指引》的通知

颁布时间：2009-11-20
发文单位：中国证券业协会

各基金销售机构：

为保护投资者的合法权益， 促进基金销售业务健康有序发展，保障基金销售机构在互联网上安全可靠地开展基金销售活动，协会组织制定了《网上基金销售信息系统技术指引》，现予发布，请参照执行。

二〇〇九年十一月二十日

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》、《证券投资基金销售业务信息管理平台管理规定》等法律法规制定本指引。

第二条 在中华人民共和国境内依法设立的基金销售机构开展网上基金销售业务适用于本指引。

基金销售机构是指依法办理基金份额认购、申购和赎回等业务的基金管理人，以及取得基金代销业务资格的其它机构，包括基金管理公司、商业银行、证券公司、证券投资咨询机构、专业基金销售机构等。

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，包括网上基金销售系统服务端、客户端和门户网站。

第四条 基金销售机构应采取技术和管理措施，保证网上基金销售系统的安全性、完整性和可用性，并做好系统信息保密工作。

第五条 中国证券业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 基金销售机构对网上基金销售信息系统应统一规划、集中管理，保证网上基金销售业务安全、有序发展。

第七条 基金销售机构应制定在网上开展基金销售业务的各项安全管理制度，对安全管理目标、安全管理组织、安全人员配备、安全策略、安全措施、安全培训、安全检查、系统建设、运行管理、应急措施、风险控制、安全审计等方面作出规定。

第八条 基金销售机构应将网上开展基金销售业务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。

第九条 基金销售机构的网上基金销售信息系统应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中国司法机构调查取证要求。

第十条 基金销售机构应当与投资者签订网上基金或网上金融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客户应采取的风险防范措施。

第十一条 网上基金销售信息系统应具有向投资者提示交易时间区间的功能。交易时间区间应严格遵守监管机构或交易所的相关规定。

第十二条 网上基金销售信息系统应由基金销售机构自主运营、自主管理。如涉及第三方（指除基金销售机构及其客户以外的任何一方），必须与第三方签订保密协议和服务协议，明确责任，采取措施防止通过第三方泄露用户信息。

第十三条 基金销售机构委托或定制开发网上基金销售业务系统，应与软件开发商签订详细的商业合同及保密协议，明确软件开发商应用软件中使用的第三方产品具备合法版权。应要求开发商提供源代码或对源代码实行第三方托管。

第十四条 基金销售机构应建立可靠的运行环境，确保基金销售系统有充足的处理能力、存储容量和通讯带宽，满足业务增长的需要。

第十五条 基金销售机构应对网上基金销售信息系统的各个子系统合理划分安全域，在不同安全域之间进行有效的隔离，保障网上基金销售前台系统与其后台系统在技术上进行有效隔离，门户网站和网上基金销售信息系统进行有效隔离。

第十六条 网上基金销售信息系统各环节必须有可靠的热备或冷备措施，保证整个系统的高可用性。

第十七条 用于网上基金销售信息系统的服务器、操作系统、平台软件等应及时进行补丁和版本升级。升级前需进行严格的系统测试。

第十八条 网上基金销售信息系统应具备 2 个或 2 个以上不同运营商的互联网接入，避免在同一运营商的线路接入上出现单点故障和瓶颈。

第十九条 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，并定期对安全日志进行检查，以提高网上基金销售信息系统的防护能力。

第三章　门户网站

第二十条 门户网站指基金销售机构建立的实现信息发布、业务咨询、营销推广、客户服务和投资者教育等功能的网站。

第二十一条 基金销售机构门户网站应在当地电信管理局办理 ICP 备案，同时向当地工商局等有关部门办理网站备案，在网站首页公布 ICP 备案号，提供客户查询门户网站备案信息的链接。

第二十二条 基金销售机构应采取有效措施监控门户网站防止被篡改。当网站上的页面内容、提供给投资者下载的客户端软件及其他文件被异常修改时，能及时发现并恢复。

第二十三条 门户网站中不得存放与基金交易业务有关的客户资料、交易数据等客户敏感数据。

第二十四条 门户网站中的客户账号及口令，应采用加密方式传输，并最低达到 SSL 协议 128 位的加密强度。

第二十五条 基金销售机构应建立对门户网站内容发布的审核、管理和监控机制，对网页内容进行监控，对有害信息进行过滤，防止网站出现不良信息。

第四章　网上基金销售信息系统客户端

第二十六条 网上基金销售信息系统客户端是指基金销售机构提供的，由基金投资人通过互联网、移动通信等非现场方式独自完成业务操作的应用系统。

第二十七条 网上基金销售信息系统客户端应能向客户提示最近一次登录的日期、时间等信息。

第二十八条 网上基金销售信息系统客户端应能在指定 的闲置时间间隔到期后，自动锁定客户端的使用或退出。

第二十九条 网上基金销售信息系统客户端的数据传输应采用国家信息安全机构认可的加密技术和加密强度，并最低达到 SSL 协议 128 位的加密强度。

第三十条 网上基金销售信息系统客户端如需与银行等支付系统进行数据通信时，应使用数字加密技术（如数字证书方式）进行严格的数据加密处理防止数据被篡改。

第三十一条 当客户访问网上基金销售信息系统时，未经客户许可，除提高安全性的控件之外，不得以任何方式在客户系统中安装插件。

第三十二条 网上基金销售信息系统应提供可靠的身份验证机制，除采用账号名、口令、验证码的身份认证方式外，还应向客户提供一种以上强度更高的身份认证方式供客户选择使用，如，客户端电脑或手机特征码绑定、软硬件证书、动态口令等认证方式，确认客户的身份和登录的合法性，防止不法分子利用木马等黑客程序窃取客户账号和口令。

第三十三条 基金销售机构为基金客户网上开立基金交易账户时，应当要求基金客户提供身份证明信息，并采取等效实名制的方式核实基金客户身份。

第三十四条 基金销售机构应采取有效技术措施，识别与验证使用网上基金销售业务服务的投资者的真实、有效身份，并应依照与投资者签订的协议对投资者操作权限、资金转移或交易限额等实施有效管理。

第三十五条 网上基金销售信息系统客户端不得在客户本地计算机储存客户账户、口令等重要信息。存储其它信息应当提示客户，本地数据存储只是参考数据，应当以基金销售机构记录数据为最终准确数据。

第三十六条 网上基金销售信息系统客户端应当具有基金客户交易口令复杂度控制和提醒机制，提醒客户定期修改口令；系统自动生成的初始口令，必须有最小生存期限制或强制客户修改，禁止系统自动生成相同口令或弱口令；基金客户口令的修改和取回操作要有日志记录。

第五章 网上基金销售信息系统服务端

第三十七条 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客户提供网上基金交易、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。

第三十八条 网上基金销售信息系统服务端应能向客户提供可证明服务端自身身份的信息，如提供预留验证信息服务，在客户登录时向客户显示预留的验证信息， 以帮助客户识别仿冒的网上基金信息系统，防止不法分子利用仿冒的网上基金信息系统进行诈骗活动或盗取用户账号、口令等信息。

第三十九条 网上基金销售信息系统应保障对客户的授权不被恶意提升或转授，防止客户访问未经过授权的数据，使用未经授权的功能。

第四十条 基金销售机构开展网上基金销售业务，需要对客户信息和交易信息等使用电子签名或电子认证时，应遵照国家有关法律法规的规定。

网上基金销售信息系统采用的认证授权和加密体系应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技术的发展，定期检查，适时调整。

第四十一条 网上基金销售信息系统未经基金销售机构授权不得与第三方进行任何形式的数据交换，并具备经过认证后仅向指定地址发送信息的功能。

第四十二条 网上基金销售机构应保证网上基金数据传输的保密性、完整性、真实性和可稽核性，对网上基金交易的客户信息、交易信息及其他敏感信息进行可靠的加密，不得存在任何中间环节对数据进行加解密处理。

第四十三条 网上基金销售信息系统服务端应能够抵御连续猜测，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，正常用户无法登录。

第四十四条 网上基金销售信息系统服务端应对异常情况进行监控，并具有相应报警功能。

第四十五条 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。

第四十六条 网上基金销售信息系统服务端应能在指定的闲置操作时间限制到期后，自动终止用户对系统的访问权。

第四十七条 网上基金销售信息系统服务端应能产生、记录并集中存储必要的日志信息，日志信息应至少包含能识别服务请求方身份的内容，如，登录终端的 IP 地址、MAC 地址、手机号码和终端特征码等，并确保数据的可审计性，满足监管部门现场检查要求及司法机构调查取证的要求。

第四十八条 网上基金销售信息系统服务端应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户端。

第四十九条 网上基金销售信息系统服务端应能够提供系统运行状况信息（如活动状态、并发在线客户数目、并发会话数目、线程数目、队列长度等）、错误信息、安全警告等。

第五十条 网上基金销售信息系统应具备防范 SQL 注入、跨站脚本、Session 欺骗、拒绝式服务攻击和缓冲区溢出等攻击的能力。

第五十一条 网上基金销售信息系统服务端对于客户口令等数据应当以密文形式存储。

第六章 安全管理

第五十二条 网上基金销售信息系统的开发、测试人员及环境应与运营人员及生产环境分离。开发、测试人员未经授权不得访问、修改非职责范围内的网上基金销售信息系统。

第五十三条 基金销售机构应对网上基金销售信息系统中包括网络安全设备、服务器以及应用系统在内的账户进行严格管理，账户权限应按最小权限原则设置，清除所有冗余、与应用无关的账户，并严格限制各管理员账户的使用，禁止用最高权限账户执行一般操作，尽量避免以最高权限账户运行网上基金销售信息系统服务端应用软件。

第五十四条 系统各级管理用户和口令应由专人负责，在系统允许的情况下，口令长度应在 12 位（含 12 位）以上，且含有字符和数字，区分大小写，并定期更改。

第五十五条 基金销售机构应定期进行网上基金销售系统的漏洞扫描和渗透测试工作，及时发现系统中存在的各种安全问题并及时修补。

第五十六条 原则上不允许通过互联网对网上基金销售信息系统（如防火墙、网络设备、服务器等）进行远程管理和日常维护等操作，对网上基金销售信息系统的访问控制应做到：

（一）关闭网上基金销售信息系统所有与业务和维护无关的服务及端口，严格控制防火墙中的权限设置，确保按“最小权限原则”进行设置；

（二）对于网上基金销售信息系统的内部访问，应严格限制访问源；

（三）特殊紧急情况下需要通过互联网进行远程操作时，应通过限制登录 IP、使用数字证书或动态口令、全程监控等措施确保安全，并在操作完成后，及时关闭相关端口。

第五十七条 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。对于防病毒软件，要保证病毒库的及时更新，定期对系统进行全面的病毒扫描。

第五十八条 基金销售机构应采取有效措施对门户网站上提供下载的网上基金客户端软件程序进行保护，客户端软件程序编译封装、形成下载文件后，对其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网站文件下载服务器。

第五十九条 基金销售机构应对网上基金销售信息系统进行实时监控，建立异常事件的甄别、报警、处理和报告机制。网上基金销售信息系统实时监控范围应包括各种安全设备、网络设备、服务器设备及操作系统、通讯线路状态、数据库、应用软件等。监控内容包括其运行状况、日志内容、安全警告等，应统一记录保存监控信息，保存期至少为 6 个月。

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关键软件的日志文件，并定期检查、审核记录。

第六十一条 基金销售机构网上销售系统开发、测试中不应当存放来自于生产系统的客户真实数据。

第六十二条 基金销售机构网上基金销售信息系统上线或重大版本升级，应进行安全测试或技术评估。

第六十三条 基金销售机构应建立严格的变更管理流程，对包括网络安全设备、服务器、应用系统等软硬件系统变更实行规范化的变更管理。因系统变更而导致的网上基金销售服务暂停，需提前向投资者公告。

第六十四条 基金销售机构应建立针对网上基金销售信息系统的配置管理制度，完整、真实地记录和反映系统所涉及的软硬件配置及相互影响关系，并保持与实际生产环境同步更新。

第六十五条 基金销售机构应制定网上基金销售信息系统的数据备份计划并落实执行，数据备份应有严格的保管、使用、检查制度。备份数据应包括：系统程序、客户数据、配置参数、系统日志、安全审计数据等信息。

第六十六条 基金销售机构在公司灾备系统和业务连续性计划中应当包括网上基金销售系统。

第六十七条 基金销售机构应建立网上基金销售信息系统应急处置组织体系，并有针对性地制定应急预案，应急预案应纳入基金销售机构的整体应急预案体系内，并按照有关规定进行演练。

第六十八条 基金销售机构应根据网上基金销售信息系统故障的影响和损失情况对应急组织体系和应急预案进行分级管理，并遵循统一领导、快速响应、协调配合、最小损失的原则。

第六十九条 基金销售机构网上基金应急预案应针对电力、通信等基础设施故障、计算机硬件或网络设备故障、操作系统或应用系统故障、操作系统或应用系统漏洞、病毒入侵、恶意攻击、误操作、不可抗力等可能的故障原因制定对应的应急恢复操作流程。

第七十条 基金销售机构销售机构在网上基金销售信息系统发生影响业务正常业务的技术故障时，应立即启动应急预案、尽快恢复交易业务运行，并按有关要求及时上报监管部门。

第七章 附则

第七十一条 本指引自发布之日起施行。