

Information Systems Security Program (NFA Interpretive Notice 9070)

Model Program Advisors, LLC (proposed) · a multi-program commodity trading advisor · mpaclient.com

INTERNAL — Sample for counsel review · October 28, 2026 · Principal: Austin Putt · SAMPLE — to be completed with the Advisor's actual people, systems, and vendors before NFA filing; not for publication

1. Purpose and approval

NFA Interpretive Notice 9070 requires each Member to adopt and enforce a written information systems security program (ISSP) reasonably designed to secure customer data and access to its electronic systems. This ISSP is approved by Austin Putt, [Managing Member], the Advisor's sole principal, who is also its designated security officer until the role is assigned to another person or an outside provider. It is reviewed at least every twelve months.

2. What the Advisor's systems are

The Advisor's own systems are small: a business email and document system ([vendor]), an accounting and invoicing system ([vendor]), a compliance file store ([vendor]), and the principal's workstations and phone. The client doorway, the replication service, the key vault, and the fee module are the platform operator's systems, provided to the Advisor under its infrastructure license; the Advisor does not host them and holds no access-key secrets. This ISSP therefore covers (a) the Advisor's own systems directly and (b) the platform's systems through the security obligations in the license and the Advisor's oversight of them (Section 7).

3. Risk assessment

The Advisor identifies these principal threats: compromise of the principal's email or doorway administrative credentials; unauthorized access to client files (identity, financial information, program elections); compromise of the platform's key vault or replication service, which could place or alter orders in client accounts; loss or alteration of records; vendor failure; and social engineering directed at the principal or at clients impersonating the Advisor. The assessment is updated annually and on any incident.

4. Safeguards — the Advisor's own systems

Multi-factor authentication on every account, with no exceptions; unique credentials per person; a password manager; full-disk encryption on every workstation and phone; automatic updates; endpoint protection; least-privilege access to the compliance file store with access logged; encrypted backups of records retained under Reg. 1.31; no client data on personal devices or consumer messaging; secure disposal of devices and media; and a written access list reviewed [quarterly] and on any departure.

5. Safeguards — the platform's systems (by license)

The infrastructure license requires the platform operator to: store access-key secrets in a hardware-backed vault with no display to any person; verify key permissions at linking and daily and disable any key with withdrawal or transfer scope; log every order and every administrative action in a tamper-evident record; segregate the Advisor's

client data from the brand's member data and from any other advisor's; encrypt data in transit and at rest; maintain its own ISSP and penetration testing; notify the Advisor of any security incident affecting its clients within [24] hours; and provide the Advisor an annual security attestation and the right to review test results. The Advisor's designated security officer reviews that attestation and the incident log [quarterly].

6. Employee and contractor training

Every person with access to Advisor systems is trained before access and annually on phishing, credential hygiene, client-data handling, and incident reporting. Training is recorded.

7. Vendor management

Before engaging any vendor that will hold or access client data, the Advisor records the vendor's security posture (certifications, incident history, contractual commitments), confirms contractual confidentiality and breach-notice terms, and reviews the relationship annually. The platform operator is the principal vendor and is managed under Section 5.

8. Incident response

On any suspected incident: contain (revoke credentials, disable affected keys through the platform, isolate devices); assess what data and which clients are affected; notify the platform operator or be notified by it; notify affected clients and connected brands promptly with what happened and what they should do (for example, rotate their venue key); notify NFA as its rules require and any regulator or state authority as breach-notification law requires; preserve logs and evidence; and record the incident, the response, and the remediation in the incident file. The principal leads the response; [outside counsel / security firm] is retained in advance for escalation.

9. Monitoring and review

The security officer reviews access logs and the platform's attestation [quarterly], tests backup restoration [semi-annually], and reviews this ISSP annually and after any incident, recording the review and any change.

Adopted by: Austin Putt, [Managing Member] · [DATE] · Next review: [DATE + 12 months].

Sample procedures prepared for counsel and the Advisor's principal. Not legal advice. Counsel must conform to current NFA rules and interpretive notices and approve before adoption.