Anti-Spam & Domain Protection Policy

I. Purpose & Scope

RCH Energy and RR Advisors, LLC (together “RCH” or the “Firm”) have established an email communication policy to ensure that the Firm adheres to best practice standards for all email communication, including email communication to existing investors and for general marketing purposes. The policy is designed to ensure that the Firm maintains compliance with the established CAN-SPAM email standard, preserves brand reputation, and strictly protects corporate domains (and subdomains) from being listed on URI real-time blocklists such as SURBL, Spamhaus DBL, and URIBL.

The policy applies to all employees and contractors communicating from RCH email servers and all outbound email traffic originating from corporate servers.

II. Consent & List Acquisition Standards

RCH has developed the following policy regarding all external email distribution lists or any email marketing or general emails sent or distributed to one or more recipient.

2.1 Explicit Opt-In Requirements

Each recipient of a bulk or automated email communication must have consented to receive email communications and have a documented legal basis prior to receiving the email communication. The Firm has identified two possible methods where emails addressed are collected and which must comply with the Firm’s email Opt-In Requirements:

- Email Opt-In Requirements:
  - *Existing Investors & Limited Partners:* Investor communications, including fund updates, financial statements, tax reporting, capital calls, and official partner notices, derive consent directly through executed Fund Offering Documents (e.g., Private Placement Memoranda), Subscription Agreements, or Investment Management Agreements (IMAs). These contacts are exempted from public web double opt-in workflows but remain governed by the Firm’s email delivery controls.
  - *General Public & Prospective Contacts (Confirmed Opt-In):* Any email from a web form or other public channels must utilize a Confirmed Opt-In (COI / Double Opt-In)

mechanisms. This requires a confirmation email, with a verification link, being sent to the email address and the verification link being accepted prior to the email address being added to an active marketing lists. Note that inbound email communications to an RCH team member requesting information about the Firm, an SMA or one of the Firm's private funds can satisfy the opt-in requirement as long as a record of the request is maintained.

- Proof of Opt-In Consent & Recordkeeping Requirements:
  - *Existing Investors:* RCH's Operations must maintain the contractual records that link the investor to their executed legal agreements, subscription document and client onboarding documents.
  - *Public Marketing Leads:* All web forms where an individual opts-in to receive email communication must also capture and store audit log information including the opt-in timestamp, IP address, and opt-in source URL for every subscriber.

2.2 Prohibited List Sourcing

RCH prohibits the following list-sourcing practices because they materially increase the spam-trap hits and complaint rates that drive domain listings on SURBL, Spamhaus DBL, and URIBL:

- Using any third-party email address is strictly prohibited. This includes email addresses that have been purchased, rented, appended, or received through co-registration.
- Automated web scraping, list harvesting, website lookup and directory mining of email addresses are strictly prohibited.
- Inbound sales prospects acquired via a third-party databases, must be verified through individual one-to-one outreach protocols. No email address can be added to an email distribution list without first collecting evidence of the "Opt-in".

2.3 Email List Hygiene & Validation

Best practices state that emails that have not demonstrated any activity or engagement for more than 180 days should be reviewed. Recipients who have not interacted with an email should go into a "review workflow" to identify if they want to continue to receive email communications.

The majority of RCH's email communication recipients are investors in the Firm's private funds or who have assets managed under a separately managed account. The Firm is required to provide investor statements, audited financials, privacy notices and other communications.

Therefore, email list hygiene protocols to send fewer communications are not applicable to the Firm and could violate certain regulatory reporting obligations as a SEC Registered Investment Adviser.

As a policy, if the Firm wishes to do a broader email marketing campaign the Firm will coordinate with compliance to evaluate and consider an email list hygiene review.

3. Infrastructure & Domain Technical Safeguards

The Firm considered implementing domain or subdomain segmentation (routing bulk/marketing email through a dedicated subdomain or separate domain, isolated from the firm's primary corporate domain) as an additional structural safeguard.

The Firm has determined that domain segmentation is not warranted at this time, given that:

- The Firm's outbound email consists primarily of investor statements, fund updates, and other investor-facing communications sent under an existing business relationship, rather than high-volume promotional or marketing campaigns;
- The Firm's sending volume and complaint-rate risk profile are low relative to the bulk-sending context in which domain segmentation is designed to add value;
- Routing investor communications through a separate marketing designated subdomain could reduce, rather than improve, recipient trust and deliverability, since such communications are expected to originate from the Firm's primary business domain.

This determination will be revisited if the Firm's email sending profile changes to substantially include non-investors/clients.

4. Content Safety, Link, & Redirect Standards

All outbound email content and associated destination URIs must undergo a review to ensure that the following protocols and controls are utilized.

- **Redirect Auditing:** Target links inside emails must point directly to RCH landing pages without passing through any third-party website, redirect or unvetted tracking gateway. Note that approved email service provider's own click-tracking domain is not considered a third-party redirect for purposes of this control as long as they have been vetted and approved as part of the Firm's Vendor Due Diligence controls (see Section 5).
- **Host Reputation:** Assets (images, hosted files, landing pages) referenced in emails must reside on RCH corporate infrastructure or on a pre-approved, enterprise-grade content delivery network (a "CDN").
- **Manual Periodic Checks of Email Domain:** On a quarterly or semi-annual basis a designated RCH team member shall run the sending domain through SURBL's lookup page, the Spamhaus DBL lookup, and URIBL's lookup, and mxtoolbox.com's blacklist checker to ensure that the sending domain has not been blacklisted.
- **Prohibition of Generic Shorteners:** Public link shorteners (e.g., bit.ly, tinyurl.com) are explicitly forbidden in outbound templates due to high blocklist correlation. Branded custom subdomains must be used exclusively.

5. Third-Party Vendor Oversight

RCH does not operate an affiliate marketing program. However, any third-party vendor that sends email on the firm's behalf or whose links appear in firm communications, including the Firm's email provider, Fund Administrator or Transfer Agent, and Website Hosting Provider represents a potential risk vector for blocklist listings.

The Compliance Teams maintains a list of all authorized and approved vendors. All vendors are reviewed prior to onboarding and undergo periodic reviews to confirm that the vendor's sending and tracking domains are not listed on SURBL, Spamhaus DBL, or URIBL. Broader vendor risk items, such as data protection and cybersecurity controls, are addressed under the Firm's separate vendor due diligence policy.

6. Unsubscribe Mechanics & Complaint Processing

RCH is committed to providing easy to use opt-out options to ensure that users who do not wish to receive general marketing email communications can unsubscribe. This is critical to mitigating spam complaints that feed into SURBL, Spamhaus DBL, and URIBL data sources. These controls include:

This section only applies to marketing and promotional email communications. It does not apply to, and does not create an unsubscribe right with respect to, investor statements, fund manager commentary, audited financials, tax reporting, capital calls, privacy notices, or other communications required to be delivered under the Firm's advisory agreements or applicable law.

6.1 One-Click Unsubscribe Protocols

- All bulk marketing messages must include RFC 8058 compliant headers:
    - Generic example: List-Unsubscribe: <https://mail.company.com/unsubscribe?id=12345>, <mailto:unsubscribe@mail.company.com>
      List-Unsubscribe-Post: List-Unsubscribe=One-Click
- In-body unsubscribe links must remain clear, visible, and legible across mobile and desktop clients.

6.2 Unsubscribe SLA & Suppression

- Unsubscribe requests must be processed in real-time and should not exceed 24 hours.
- The Opt-out user experience should not require user login, password entry, or secondary confirmation questionnaires.

7. Monitoring, Incident Response, & Enforcement

In the event a domain or IP is listed on SURBL, Spamhaus DBL, or URIBL, the following escalation procedures execute immediately:

1. **Immediate Pause:** Active sends referencing the listed domain or subdomain are paused as soon as practicable by the designated Compliance/IT lead upon confirmation of the listing.
2. **Root Cause Analysis:** The designated Compliance/IT lead identifies the source campaign, list, or compromised account as soon as practicable, and in any event within 3 business days.
3. **Remediation & Delisting:** Source vulnerabilities are isolated, list cleanup executed, and formal delisting requests submitted to the relevant list (SURBL, Spamhaus DBL, or URIBL) with proof of corrective action.

Last Reviewed: September 2026

4. **Enforcement Action:** Any internal employee or third-party partner found violating this policy will face disciplinary action up to termination of employment or contract.

Last Reviewed: September 2026