AI Usage Policy – Internal Guidance and Governance

Purpose and Scope

This policy outlines the appropriate and responsible use of artificial intelligence (AI) tools and systems within the organization. It applies to all employees, contractors, and third parties using AI tools for work-related tasks. The policy aims to ensure AI is used ethically, securely, and in compliance with laws and industry standards, minimizing reputational, legal, and operational risks.

Permitted AI Use Cases

AI must not replace human judgment. All AI outputs must be reviewed and validated before use in decisions, communications, or business processes. Employees are fully responsible for the accuracy and compliance of final work products.

AI tools may support:

- Research and analysis
- Content generation (for internal use only)
- Process automation and internal support
- Communication assistance

General Use Requirements

AI tools are provided to support business functions and productivity within the scope of each employee's role. Users should refrain from using AI systems for purposes unrelated to their assigned job duties. This includes—but is not limited to—using AI tools to self-diagnose or attempt to repair computer or application issues. AI tools should not be used as substitutes for internal support services, established procedures, or professional expertise provided by designated departments.

Additional Considerations:

- Only use company-approved AI tools.
- Never input confidential, proprietary, or sensitive data into AI systems unless explicitly approved by IT and Compliance leadership.
- Verify the accuracy of AI-generated outputs against reliable sources.
- Do not use AI tools to draft legal documents or third-party contractual content.
- Avoid using AI in a manner that violates privacy, intellectual property, anti-discrimination, or other applicable laws and regulations.

Responsibilities and Oversight

- IT and Compliance teams review and approve AI tools before organizational use.
- Managers assist in determining appropriate use cases aligned with business goals.
- Users must exercise critical judgment and report concerns or misuse.

Fund Management Specific Requirements

For fund-related activities, AI-generated outputs must:

- Be reviewed by the Chief Compliance Officer prior to use in investment decisions or client-facing materials.
- Be supported by verifiable sources and documented appropriately.
- Comply with all regulatory standards and adhere to human fiduciary judgment and due diligence.

Data Access and Security

- Access AI systems only within your authorized permissions.
- Do not view, share, or use unauthorized data. If accidentally accessed, report immediately to IT.
- Use strong credentials or company standard single sign-on for system access.
- Handle personal data in compliance with data protection laws and internal privacy policies.

Incident Reporting and Feature Requests

- Report unauthorized access to the IT team immediately.
    - If access is related to Fund Management also report to Chief Compliance Officer.
- IT will assess requests based on security, compliance, and business value.

Risk Awareness

AI technologies introduce specific risks that the Firm must identify, assess, and mitigate as part of its risk management program. The following AI-specific risk areas have been recognized, along with strategies to control or reduce them.

- Bias, Discrimination, and Hallucinations: AI tools may reflect bias or produce inaccurate or fabricated (hallucinated) content. Mitigation: Review outputs for fairness and accuracy. Use diverse data, apply human oversight, and verify content before use.
- Risk: AI-generated content may contain errors or fail to meet organizational standards. Mitigation: Users are responsible for correcting errors and ensuring all content aligns with organizational requirements.
- Overreliance on AI may reduce critical thinking or bypass necessary human judgment. Mitigation: AI outputs should support—not replace—professional expertise. Final decisions remain the responsibility of the user.
- Use of unapproved AI tools may lead to data leaks or exposure of sensitive information. Mitigation: Only approved AI tools may be used. Users must follow data protection policies and ensure tools meet security and compliance standards.

Violations and Consequences

Violation of this policy may result in disciplinary action which may include termination for employees and contractors; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of Northmarq Information Technology resources access privileges, civil, and criminal prosecution. The company reserves the right to audit AI use and investigate incidents.

Questions and Support

Users should consult managers or the IT support team when unsure about appropriate AI use.