

Anti-Money Laundering and Counter-Terrorist Financing Policy

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the “Policy”) outlines Nodemark Solutions (the “Company”) approach to preventing money laundering and the financing of terrorism within the Company’s operations. As a company providing liquidity solutions, consultancy, and marketing for Web3 projects, we recognize the unique challenges and risks this space presents. The goal of the Company is to operate transparently and responsibly while supporting the growth of the decentralized ecosystem. The safety and protection of the clients, employees, and all those connected to the Company is a top priority. We also provide cooperation and support to government authorities, law enforcement, and regulatory agencies in their efforts to prevent and tackle financial crime. This cooperation underscores our responsibility to support a stable and compliant framework.

We regularly assess the potential risks connected to money laundering and terrorist financing across all areas of our business. This process starts with getting a clear picture of who our clients are, their background, business activities, and how they intend to use our services. We also look closely at the types of transactions we handle which can sometimes present higher risks. Additionally, we take into account the geographic locations involved, since some jurisdictions carry more regulatory or reputational risk than others. When we identify clients, transactions, or jurisdictions that pose a greater level of risk, we apply more thorough checks and ongoing monitoring to reduce the chances that our services could be exploited for illegal purposes. This layered approach helps us stay alert to new threats and adapt quickly as the environment changes.

Before engaging in any business relationship, we take steps to confirm who our clients are. The depth of these checks depends on the level of risk each client presents. For standard-risk clients, this might involve collecting basic identification information, such as but not limited to, government-issued IDs or company registration details. For higher-risk clients, we go further by asking for additional documents that clarify where their funds come from and how their business operates. This helps us make sure that the source of their assets is legitimate and that their activities align with what they have shared to us. The goal is to have a clear understanding of each client to avoid any connections to illicit activities.

We keep an eye on all transactions and activities that go through our services to spot anything unusual or out of the ordinary. This includes looking for patterns that do not match what we typically see from a client’s normal behavior, such as sudden large transfers, unexpected changes in transaction frequency, or transactions involving high-risk jurisdictions. When something seems off or raises concerns, it is flagged for immediate review. This process helps us catch potential risks early and take appropriate action to prevent misuse of our platform.

When we come across any activity that appears suspicious or does not align with expected behavior, we report it promptly to the appropriate regulatory or law enforcement authorities,

following all applicable laws and guidelines. We understand the importance of transparency in these situations and work closely with the authorities, providing any information or documentation they need. Our cooperation extends through any audits or inquiries to support efforts to combat money laundering and terrorism financing effectively.

We maintain detailed records of client identification, transaction histories, and any reports related to suspicious activity for a minimum of five years. Keeping these records helps create a clear audit trail and supports transparency, making it easier to review past activities if needed. This approach strengthens accountability and aligns with legal and regulatory requirements. At the same time, we handle all personal and business information with strict confidentiality, following our Privacy Policy. Data collected is stored securely and accessed only by authorized personnel, ensuring it is protected against unauthorized use or disclosure.

This streamlined version of our Policy provides an overview of our approach and core principles related to Anti-Money Laundering and Countering the Financing of Terrorism. Please note that specific operational details and internal procedures are excluded to maintain security and comply with regulatory requirements.

This Policy will be reviewed and updated regularly to keep pace with changes in laws, regulations, and emerging risks. We adapt our approach as the regulatory landscape and business environment evolve to stay aligned with best practices and maintain effective safeguards.