Confidentiality and Data Privacy Policy

Document Version: 1.0
Date: August 1, 2025
Prepared for: Atlas Labs FZE, Dubai Entity

1. Introduction and Scope

This policy outlines Atlas Labs FZE's commitment to protecting confidential information and personal data, as mandated by the **VARA Technology and Information Rulebook - Rule III.A** (Use and protection of confidential information) and **Rule II.B** (Data Privacy Compliance Programme). This policy applies to all employees, contractors, and third-party service providers who handle confidential information or personal data on behalf of Atlas Labs FZE.

2. Confidential Information

2.1. Use and Protection of Confidential Information

Atlas Labs FZE implements the following measures to protect the confidentiality of all client-related information and records:

- **Confidentiality Agreements:** All employees, contractors, and third-party service providers are required to sign a confidentiality agreement before being granted access to any confidential information. These agreements explicitly outline the purpose for which the information can be used and the prohibition against unauthorized use or sharing.
- **Role-Based Access Controls:** Access to confidential information is strictly limited to individuals who require it to perform their official duties. Our IT systems enforce role-based access controls, and access is provisioned and revoked as part of our formal onboarding and offboarding procedures.
- **Staff Certification and Training:**
    - All staff undergo mandatory training on our internal policies for the collection and processing of confidential information during their initial onboarding.
    - Compliance with these policies is periodically certified by each staff member, and we maintain records of this certification for a period of eight years.
- **Prohibition on Unauthorized Sharing:**
    - Confidential information can only be shared internally or with other entities if it is **absolutely necessary** for conducting VASP activities.
    - Under no circumstances may confidential information be used for the purpose of trading Virtual Assets by any entity, including Atlas Labs FZE and

its staff. This is monitored through our transaction monitoring systems and internal audits.

2.2. Provision of Information to VARA

In compliance with **VARA Technology and Information Rulebook - Rule II.C**, Atlas Labs FZE will:

- **Full Access:** Take all necessary steps to ensure VARA has full access to any information related to our compliance with data privacy regulations, regardless of where the information is stored. This includes providing notifications, contractual provisions, and obtaining all necessary consents.
- **Timely Reporting:** Provide access to this information in the manner and within the timelines communicated by VARA.
- **Data Incident Notification:** Notify VARA within **24 hours** of any incident affecting or potentially affecting personal data. A summary of the report to the data regulator will be provided to VARA, along with a full copy if the data regulator is in the UAE, unless legally prohibited.

3. Data Privacy Compliance

In accordance with **VARA Technology and Information Rulebook - Rule II.B**, Atlas Labs FZE has established a written data privacy compliance program with the following key measures:

- **Data Protection Officer (DPO):**
  - We have appointed a **Data Protection Officer** who possesses the appropriate competencies and experience as per the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data (PDPL).
  - The CISO and the DPO roles may be held by the same individual to ensure a cohesive approach to both data security and privacy.
- **Privacy Management Function:**
  - A dedicated function within the organization is responsible for the ongoing management and protection of personal data.
  - This function is responsible for implementing and maintaining our privacy processes, procedures, and controls.
- **Third-Party Oversight:**
  - We conduct due diligence on all third-party service providers to ensure they have adequate data protection measures in place.
  - Our contracts with these providers include clauses that require them to comply with all applicable data protection laws.

- **Employee Training:**
  - All staff receive mandatory training on data privacy laws and our internal policies during onboarding and annually thereafter.
- **Data Breach Protocol:**
  - Our **Business Continuity and Disaster Recovery Plan** includes a specific protocol for data breaches.
  - This protocol outlines the steps to be taken to identify, contain, and mitigate the impact of a breach, including the notification process for affected clients and relevant authorities, including VARA.

4. Policy Review and Updates

This policy will be reviewed and updated at least annually by the CISO and the Compliance Officer to ensure it remains compliant with all applicable laws and best industry practices. Any material changes will be communicated to all staff, and their acknowledgment of the new policy will be documented.