



Anti-Money Laundering Policy



## **Introduction**

Money laundering poses a significant threat to the integrity of the financial system and the overall economic stability of India. As a responsible corporate entity, InfoBeans recognizes the importance of implementing effective Anti-Money Laundering (AML) measures to mitigate the risk of being involved in money laundering activities. This policy serves as a framework to guide our employees, agents, contractors, and associated entities in complying with AML regulations and fostering a culture of transparency, accountability, and ethical business conduct. InfoBeans enforces an absolute zero-incident benchmark for AML incidents.

### **1. Objective**

The objective of this AML Policy is to establish a robust framework to:

- Prevent the use of the company's products, services, or facilities for money laundering or terrorist financing activities.
- Comply with all applicable AML and CFT(Combating the Financing of Terrorism) laws, regulations, and guidelines in India.
- Detect, report, and mitigate any suspicious activities related to money laundering or terrorist financing.
- Train and educate employees on AML and CFT policies, procedures, and best practices.

### **2. Scope**

This AML policy applies to all employees, directors, officers, and agents of InfoBeans, as well as any associated entities and third parties acting on behalf of the company.

### **3. Compliance with Applicable Laws and Regulations**

InfoBeans shall adhere to all relevant laws and regulations related to AML in India, including but not limited to:

- The Prevention of Money Laundering Act, 2002, and subsequent amendments.
- The guidelines issued by the Financial Intelligence Unit-India (FIU-IND).
- The regulations prescribed by the Reserve Bank of India (RBI) and other relevant regulatory authorities.

## **4. AML Program**

### **4.1. Risk Assessment**

InfoBeans shall conduct a comprehensive risk assessment to identify, assess, and understand the potential risks of money laundering associated with its business operations, customers, products, services, and geographical locations. The risk assessment shall be periodically reviewed and updated to reflect changes in the risk landscape.

### **4.2. Customer Due Diligence (CDD)**

#### **4.2.1. Know Your Customer (KYC)**

InfoBeans shall establish robust KYC procedures to verify and identify customers, beneficial owners, and authorized signatories. The KYC process shall involve collecting relevant customer information, such as identification documents, proof of address, and other necessary details, as per regulatory requirements.

#### **4.2.2. Enhanced Due Diligence (EDD)**

For higher-risk customers or transactions, InfoBeans shall implement enhanced due diligence measures, including obtaining additional information, conducting source of funds inquiries, and performing ongoing monitoring.

### **4.3. Reporting and Record Keeping**

InfoBeans shall maintain accurate records of all customer transactions, including supporting documents, for the prescribed periods as per regulatory requirements. The company shall promptly report suspicious transactions to the appropriate regulatory authorities as mandated by the law.

### **4.4. Employee Training**

**a.** InfoBeans will provide regular training and awareness programs to employees, contractors, and stakeholders to ensure their understanding of AML and CFT policies, procedures, and their roles in preventing and detecting money laundering and terrorist financing activities.

**b.** Training programs will cover topics such as customer due diligence, recognizing suspicious activities, reporting obligations, and legal obligations under AML and CFT laws.

### **4.5. AML Compliance Officer**

The company shall designate an AML Compliance Officer responsible for overseeing the implementation and effectiveness of the AML program, including monitoring transactions, conducting internal audits, and ensuring compliance with applicable laws and regulations.

**a) Reporting and Whistleblowing**

InfoBeans encourages employees and stakeholders to report any suspected or known instances of money laundering or suspicious activities through designated reporting channels. Whistleblowers shall be protected from any retaliation or adverse consequences resulting from their reporting.

**b) Internal Controls and Monitoring**

InfoBeans shall establish internal controls, policies, and procedures to monitor and mitigate the risk of money laundering effectively. This includes the use of automated systems, transaction monitoring tools, and periodic internal audits to identify and report any suspicious activities.

**c) Non-Compliance and Disciplinary Actions**

Non-compliance with this AML policy, applicable laws, and regulations shall result in appropriate disciplinary actions, which may include warnings, retraining, suspension, termination, or legal proceedings, depending on the severity.

**5. Policy Review:**

This AML Policy will be reviewed periodically, or as required, to ensure its effectiveness and compliance with evolving laws and regulations. Any necessary updates or amendments will be communicated to all relevant stakeholders.

By implementing this AML Policy, InfoBeans is committed to creating a secure and transparent environment that protects its business operations, stakeholders, and the financial system from the risks of money laundering and terrorist financing.