ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING, AND KNOW YOUR CLIENT POLICY

The purpose of the GXO (hereinafter referred to as the "Company" or "GXO") Anti-Money Laundering, Counter-Terrorist Financing, and Know Your Client Policy (hereinafter — the "AML/CTF and KYC Policy") is to identify, prevent, and mitigate possible risks of GXO being involved in illegal activities.

To comply with international and local regulations, GXO has implemented effective internal procedures to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption, and bribery. Additionally, GXO is committed to responding appropriately to any form of suspicious activity from its Users.

Anti-Money Laundering (AML) refers to the laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income. Combating the Financing of Terrorism (CFT) is a set of government laws, regulations, and other practices that are intended to restrict access to funding and financial services for those whom the government designates as terrorists. By tracking the sources of funds that support terrorist activities, law enforcement agencies may be able to prevent some of these activities from occurring.

All firms must adhere to the Money Laundering and Terrorist Financing regulations, as well as the recommendations from the Financial Action Task Force (FATF) — an inter-governmental body that develops and promotes national and international policies to combat money laundering and terrorist financing.

AML/CTF and KYC Policy Includes:
- Verification procedure
- Compliance Person
- Transaction Monitoring
- Risk Assessment
- Risk Categories

VERIFICATION PROCEDURE

To combat the funding of terrorism and money laundering, the law requires all financial institutions to obtain, verify, and record information that identifies each person or entity opening an account. GXO is legally required to collect the following details before approving any Account:
- Name, address, and date of birth
- Information about the User's organization (if applicable)
- Other personal or business details that confirm identity

Users may be required to submit official identification documents, such as:
- A driver's license or passport
- An organization's articles of incorporation

• Bank statements or utility bills to verify address

GXO may also obtain credit and other consumer reports to assist in verifying the User's identity. If the required information and documentation are not provided, GXO may not be able to open the account.

By applying for a GXO Account, Users agree to provide the requested information and documentation, and consent to GXO acquiring credit and other reports to verify their identity.

The Customer Due Diligence (CDD) procedure requires Users to provide reliable, independent source documents to confirm their identity and residential address. This may include:
• National ID card or international passport
• Bank statements or utility bills

GXO reserves the right to:
• Collect and verify User identification information in accordance with its AML/CTF and KYC Policy
• Authenticate documents and verify User identity through secondary sources
• Conduct ongoing monitoring of User identity and transactions, particularly if changes occur or if the User's activities appear suspicious
• Request updated identification documents when necessary

User identification information will be collected, stored, and protected in compliance with the GXO Privacy Policy and relevant regulations. Users must notify GXO of any changes to their information that may affect their account.

If a User's identity cannot be confirmed, or if their activities are suspected to be illegal, GXO reserves the right to deny or terminate services.

To ensure the legitimacy of funds, GXO may request evidence of the source of funds, including:
• Bank statements for fiat money transactions
• A video verification of wallet transactions for cryptocurrency transactions

Users who intend to use payment cards must undergo an additional verification process as outlined on the GXO website.

Additionally, GXO uses independent third-party companies to:
• Check Users against Politically Exposed Persons (PEP) and Sanctions Lists
• Assess Users' cryptocurrency wallets for AML compliance

If third-party analysis determines that a User is associated with high-risk wallets, GXO reserves the right to terminate or refuse the account.

THE COMPLIANCE PERSON

The Compliance Person is an individual duly authorized by GXO, responsible for ensuring the effective implementation and enforcement of the AML/CTF and KYC Policy.

The Compliance Person's responsibilities include:
• Collecting and verifying User identification information
• Developing and updating internal policies and procedures
• Monitoring transactions and investigating suspicious activities
• Maintaining a records management system for compliance documentation
• Communicating with law enforcement agencies when required

The Compliance Person acts as the primary contact for law enforcement in cases related to money laundering, terrorist financing, and other financial crimes.

TRANSACTION MONITORING

Before engaging in transactions, all GXO Users must complete identity verification. Once verified, the User consents to transaction monitoring.

GXO utilizes data analysis tools to:
• Identify transactional patterns
• Detect suspicious activity
• Maintain compliance records

To prevent illicit activities, GXO will:
• Monitor all transactions and report suspicious activity to law enforcement
• Request additional documentation for transactions flagged as suspicious
• Suspend or terminate accounts if reasonable suspicion of illegal activity exists

The Compliance Person regularly reviews transactions to determine if they need to be reported as suspicious.

RISK ASSESSMENT

The European Union has implemented strong legislation to combat money laundering and terrorist financing. The European Commission ensures effective compliance with these laws. International organizations, including MONEYVAL and FATF, continuously assess money laundering and terrorist financing risks.

To comply with AML and CTF obligations, GXO conducts an annual AML Risk Assessment to:
• Identify potential money laundering risks
• Evaluate AML controls in place
• Establish residual risks that require further mitigation

The Compliance Person is responsible for managing financial crime risks and improving risk management strategies.

RISK CATEGORIES

1. Risk by Users

Users may be classified as high risk due to:
• Suspicious documentation (e.g., fake IDs, stolen identities)
• Criminal background (e.g., previous financial crimes, links to terrorism)
• Inconsistent personal or business information

Additionally, Politically Exposed Persons (PEPs) — such as government officials, senior executives, or military officers — are subject to enhanced due diligence.

2. Risk by Countries

The EU Directive (EU) 2015/849 and 5th AML Directive (EU) 2018/843 identify high-risk third countries with weak AML/CTF regulations.

For business relationships involving these jurisdictions, GXO requires additional due diligence, including:
• Collecting more detailed User information
• Investigating the source of funds
• Obtaining senior management approval

FINAL REMARKS

GXO is committed to maintaining the highest standards of compliance, transparency, and risk management to prevent financial crimes. The AML/CTF and KYC Policy will be reviewed and updated regularly to ensure compliance with international regulations and emerging threats.