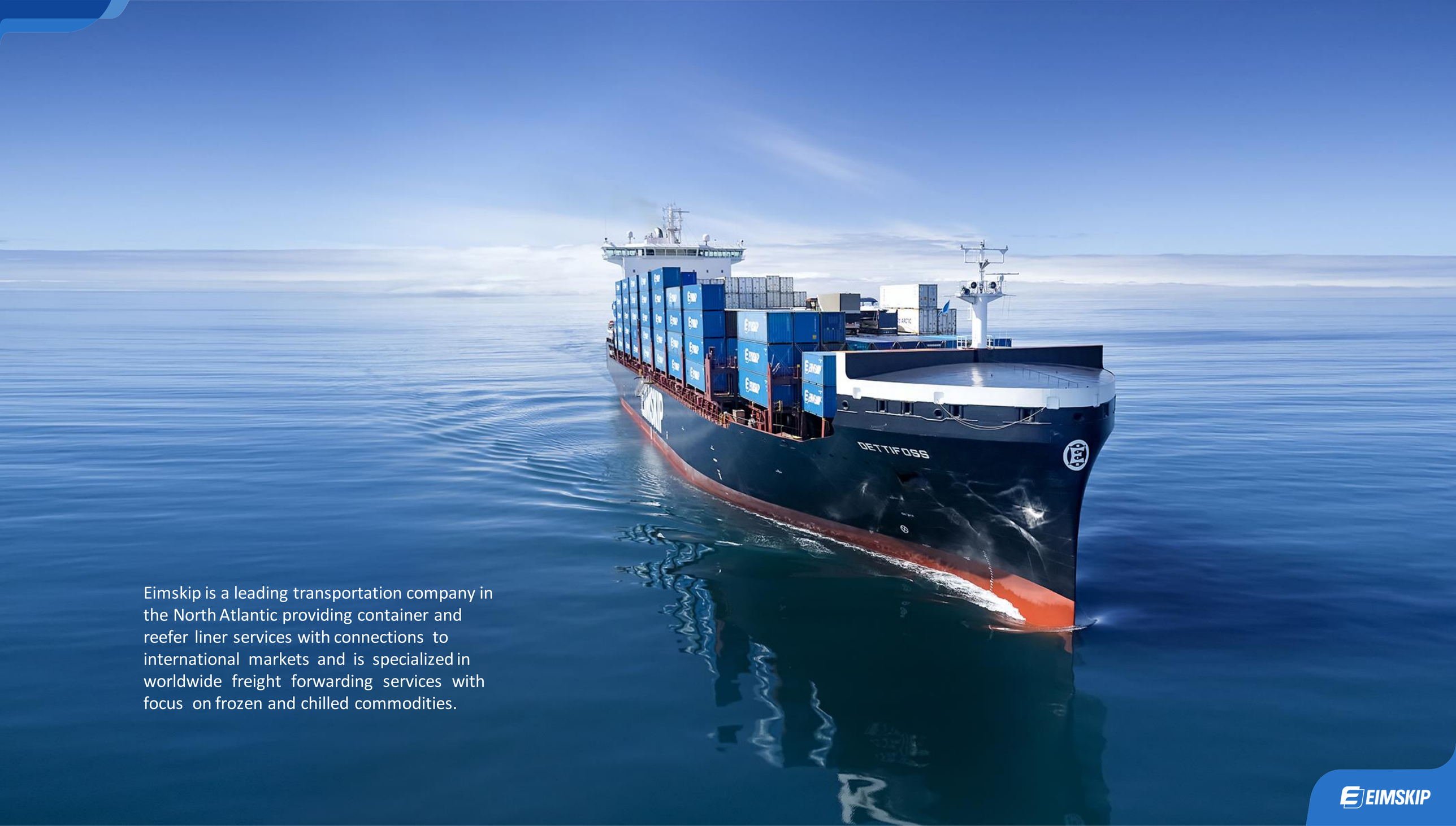
EIMSKIP GROUP

ANTI-MONEY LAUNDERING AND SANCTION POLICY



Eimskip is a leading transportation company in the North Atlantic providing container and reefer liner services with connections to international markets and is specialized in worldwide freight forwarding services with focus on frozen and chilled commodities.

OUR VALUES

ACHIEVEMENT

We simplify things for our customers. That’s how we achieve our goals.

COOPERATION

We offer outstanding solutions and services. We do that through cooperation.

TRUST

We show responsibility towards customers, share- holders, society, and the environment. That's how we earn trust.

INTRODUCTION

This policy applies to all employees of Eimskipafélag Íslands hf. and all companies within Eimskip Group

PURPOSE

Eimskip is committed to conducting all its business in a lawful, honest, and ethical manner as outlined in the Company's Code of Conduct. This policy supports integrity by prohibiting any employee of Eimskip from participating in money laundering, terrorist financing, and sanction breaches.

Each employee subject to this policy is expected to know and comply with all applicable money laundering and terrorist financing laws and regulations, as well as applicable sanctions.

DEFINITION

MONEY LAUNDERING:

Money laundering is the process by which individuals or entities attempt to conceal the origins, ownership, or control of funds obtained through illegal activities. This is typically achieved by passing the illicit funds through a complex series of transactions or financial instruments to make them appear legitimate. The goal of money laundering is to integrate the illicit funds into the legitimate economy

TERRORIST FINANCING

Terrorist financing refers to activities that provide financing or financial support to terrorists. Transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering. It may involve funds raised from legitimate sources, such as personal donations, profits from businesses and charitable organizations.

GLOBAL SANCTIONS REGIMES

Global Sanctions Regimes are political and economic decisions that are a part of diplomatic efforts by countries, and multilateral or regional organizations against states or organizations, either to protect national security interests or to protect international law and defend against threats to international peace and security.

FINANCIAL ACTION TASK FORCE (FATF)

Is the global money laundering and terrorist financing watchdog. The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that are issued three times a year.

1. The first public document, the statement "High-Risk Jurisdictions subject to a Call for Action" (previously called "Public Statement"), identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country. This list is often externally referred to as the “black list”.
2. The statement "Jurisdictions under Increased Monitoring" (previously called "Improving Global AML/CFT Compliance: On-going process”) identifies countries that are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the “grey list”.

CUSTOMERS DUE DILIGENCE

Employees must have adequate knowledge of customers, including familiarity with their identity:

- Employees should understand the purpose of the legal entity and its beneficial owners.
- Employees should identify the purpose and nature of the business relationship.
- Employees should also ensure that people representing customers have the proper authority to do so and if they are politically exposed persons (PEP).
- Employees should show special caution regarding customers who are in high-risk areas. One measure of high-risk areas is to follow FATF-listed countries updated every 4 months.

ONGOING MONITORING

Employees should try to keep information on customers up to date. Information should be updated on a regular basis and employees should update information if they notice it is incorrect or insufficient. Employees should also check the current information, for example when changes are made to the business relationship or if the customers ask for additional services. Employees should endeavour to understand the nature and purpose of the transactions they are responsible for supervising and be alert to changes in trading patterns which may indicate a change in the nature of the business relationship.

BE ALERT

Employees should always be alert to unusual or suspicious transactions or conduct by customers and notify the Legal & Compliance division of any suspicion they may have that transactions may be linked to actions punishable by law, without letting the customer or a third party know that they have notified the incident.

MONITORING

Eimskip can determine customer risk levels with screening tools when opening a customer account for accurate risk assessment. Employees can use screening tools for new and current customers in comprehensive global sanctions, PEP, and adverse media data.

SCREENING TOOLS

Screening will be conducted on high-risk customers against relevant sanctions lists issued by international bodies, governments, and regulatory authorities.

The list mentioned below is by no means exhaustive:

CREDITINFO

UK CONSOLIDATED LIST

EU CONSOLIDATED LIST

EU COUNCIL REGULATION 833/2014

EU SANCTIONS

US OFAC (SANCTIONS)

OFAC-SPECIALLY DESIGNATED

OFAC-SANCTIONS LIST SEARCH

RECORD OF SCREENING

When a customer is screened, a written record needs to be kept. A screening template is available for employees where relevant information needs to be registered, sources used for screening and date of screening.

ONGOING MONITORING

It is important to screen the customer again when circumstances change. For example

- An individual changes their name
- There's a change in the beneficial ownership of a customer
- The customer you about a transaction that is not consistent with your knowledge about them. instructs

EMPLOYEES RESPONSIBILITIES AND PROHIBIT ACTONS

EMPLOYEES SHOULD:

- Know their business partners. That means they need to do appropriate due diligence and screening of customers to ensure that they do not participate in money laundering or terrorist financing and that no sanctions have been enforced on the country, organization, and/or individuals.

EMPLOYEES CAN NOT:

- Participate in money laundering in any form.
- Participate in terrorist financing in any form.
- Do any business where sanctions have been enforced on countries, regimes, organizations, and/or individuals.

TRAINING AND AWARENESS

The Company will provide training to employees to ensure they understand their obligations under this AML and Sanctions Policy and relevant laws and regulations. Employees should be trained to perform due diligence, and recognize the signs of money laundering, terrorist financing, and sanctions violations, and understand the importance of compliance in preventing financial crimes.

Employees should receive appropriate training when changes to the relevant rules or procedures occur. This training should ensure that employees know their and the company's obligations with respect to measures against money laundering and terrorist financing and the consequences of failing to keep these obligations.

VIOLATIONS

Non-compliance with this policy may result in disciplinary action, including termination of employment or termination of business relationships. The Company is determined to apply this policy to uphold the integrity of the operation and prevent financial crimes and breaches of sanctions.

REPORT SUSPECTED OR ACTUAL VIOLATIONS

If an employee suspects breaches or misconduct within the Company's operations, it should follow the protocol of the Whistleblower Policy. Employees who make such reports in good faith will be protected from any retaliation.

.

REVIEW

Legal & Compliance division is responsible for Eimskip's Anti-Money Laundering and Sanction Policy and will initiate audits of it every two years or when necessary.

Approved by the Executive Board of Eimskipafélag Íslands hf. Reykjavík, February 16th, 2021, updated May 7th 2024.

EIMSKIP