COUNTERPARTY DUE DILIGENCE: KNOW YOUR CUSTOMER ("KYC") POLICY

Introduction

This KYC policy (the "**Policy**") applies to ArrowResources AG ("**ArrowResources**") and its affiliated companies (collectively the "**Group**"). This Policy aims to provide guidance to every employee, director, and officer in each Group company and in every joint venture company under ArrowResources' control (each an "**Employee**" and collectively the "**Employees**"). Contractors and consultants who are working on our behalf or in our name will be required to act consistently with this Policy. ArrowResources maintains a compliance team in London and Steinhausen, with regional compliance desks as required (the "**Compliance Department**"). The Compliance Department's main tasks are:

- to establish a robust compliance programme (the "**Programme**");
- to ensure that all Employees abide by the Programme;
- to prevent any breach of the Programme; and
- to provide regular mandatory and supplementary training on the subject to all Employees.

The Policy is a cornerstone of the Programme. The Compliance Department controls and coordinates the KYC approval process **from and to all Group counterparties**.

Scope

This Policy is an ongoing, risk-based process to collect, verify and monitor information about the Group's counterparties, including their identity, legal status and business activities. This Policy aims to achieve the following compliance objectives:

- to maintain a reliable database of verified and up-to-date information about all counterparties;
- to ensure compliance with all applicable economic, sectoral, financial or trade sanctions laws, rules and regulations;
- to ensure compliance with all other applicable laws, rules and regulations not least as regards Anti-Money Laundering, Anti-Bribery, etc; and
- to establish a fundamental practice to protect the Group in respect of all the above including from fraud, losses, possible fines and sanctions.

Knowledge about our counterparties is a fundamental code of behaviour that applies to everyone. It is valid for Employees at all levels, in all parts of the Group. Only by strictly adhering to this Policy we can avoid significant legal, default and other risks to the Group and its activities.

This Policy, together with the Group's detailed KYC procedure (the "**KYC Procedure**"), is instrumental in identifying key details of the Group's counterparties, including but not limited to their (beneficial) owners, senior management, sanctions and trade compliance issues, regions of operation and internal controls. The data is collated and reviewed by the Compliance Department and verified by independent external sources to identify any possible compliance issues.

All Group companies can only enter transactions with approved counterparties. All counterparties require authorisation from the Compliance Department to ensure that entering a business relationship with them does not expose the Group to any illegal, improper or undesirable activities in strict compliance with the orders of the Board of Directors of ArrowResources, the Code of Conduct, other relevant Group policies/regulations and all applicable laws and regulations. Commercial transactions can only be entered into with approved counterparties.

Due diligence check and approval

Step 1: Introduction of counterparty

The Employee responsible for the counterparty relationship (e.g. a trader, head of the relevant desk, the CEO, the CFO, the COO, Head of Trade Finance, Head of Accounting, Head of Operations, General Counsel, etc) (the "**Responsible Employee**") will (i) introduce the Compliance Department to the counterparty and (ii) provide the Compliance Department with the relevant contact details of the counterparty responsible for providing the relevant KYC information.

The Compliance Department will send the counterparty a KYC questionnaire and it will then review the information provided in that form, together with any additional information provided by the counterparty. The key objective of the first step is to collect information about the counterparty which is sufficient for the purposes of:

- identification by its name and registered address;
- understanding its current legal status;
- understanding its ownership structure and ultimate beneficial owner(s); and
- defining authorised individuals to conclude business and enter transactions with the Group.

For the purpose of ascertaining a counterparty's identity, the Compliance Department will request from relevant counterparties copies of all documents mentioned in the KYC Procedure (which include but are not limited to the counterparty's corporate and constitutional documents, ultimate beneficial owner(s), relevant officer(s) and director(s), etc).

Step 2: Review of counterparty

The Compliance Department will then verify that information through publicly available sources and also through independent external information service providers (e.g. Dow Jones and Bureau Van Dijk).

If there is a lack of information or any irregular details are revealed by the investigation, the Compliance Department will require clarification(s) from the counterparty and will accordingly review such information and/or request additional information from the counterparty until it is able to make its decision.

The Compliance Department will also determine whether the counterparty is suitable for the simplified due diligence process or the enhanced due diligence process in accordance with the KYC Procedure. If the latter, additional verification and/or information will be requested from a counterparty and/or

external sources where they are deemed to represent a higher level of risk. The Compliance Department maintains a risk assessment and ranking of all counterparties.

Step 2 will lead to a formal decision by the Compliance Department.

Step 3: Decision regarding counterparty

Upon completion of the KYC approval process under step 2, the Compliance Department will make a formal decision regarding the counterparty. This will be communicated to the Responsible Employee, and will be one of the following:

(a) approved without restrictions; or
(b) approved but with restrictions (to be listed); or
(c) not approved (If the counterparty is found not to be an acceptable counterparty the Responsible Employee will be advised by the Compliance Department and given the reason(s) which prevented the approval.)

The decision will also be communicated, where applicable, to the relevant line manager, Finance and/or Credit department as may be required. If any restrictions are levied, they will also be communicated, in addition to being entered on to the central database.

If, following approval, a significant change occurs to the counterparty including but not limited to:

- a change of ownership/ senior management or financial standing;
- a reported violation by the counterparty of any compliance requirement;
- a reported or potential violation of any applicable law, rule or regulation; and/or
- serious concerns are raised by another desk, e.g. Credit, Risk, Operations or Tax,

then the originally given approval may be temporarily suspended and/or withdrawn by the Compliance Department pending and/or following any investigation by the Compliance Department.

Ongoing monitoring

Counterparties deemed as high risk on the initial risk assessment shall be subject to a renewed compliance check between 6 and 18 months as the Compliance Department may determine. All other existing counterparties are subject to a renewed compliance check by the Compliance department under the Policy on a progressive basis, with the aim that approximately every two years each counterparty will undergo a renewed compliance check, and only if this is passed will they be permitted to remain as an approved counterparty.

Possible adverse effects of non-compliance

Non-compliance with this Policy may lead to the following adverse consequences:

- default and/or termination of commercial contracts, derivative transactions and other financing or commercial arrangements;

- damages and/or losses due to significant fines imposed on the Group by regulatory and/or supervisory bodies and/or government authorities;
- blocking of funds of the Group's accounts with credit institutions as a result of doing business with the counterparties which are subject to any economic, sectoral, financial or trade sanctions laws, regulations, adopted, enacted or enforced by any judicial or administrative authority and/or as a result of contracting with such prohibited entities;
- withdrawal of credit lines, financing lines and an inability generally to conduct business in the ordinary course; and
- reputational damage to the Group in relation to the above.

Internal controls

The following controls help protect the Group from potential adverse consequences:

Monitoring and evaluation

The Compliance Department shall (i) monitor and update this Policy from time to time in accordance with applicable laws, rules and regulations and to ensure that it remains useful, relevant and up-to-date; and (ii) ensure that the Group's policies, procedures, and internal controls are effective at preventing and detecting any violation of applicable laws, rules and regulations.

Information, confirmation and training

The Compliance Department shall provide training on this Policy to relevant Employees both at the outset of their employment with the Group, and on an ongoing basis. All training records are monitored and tracked by the Compliance Department who also ensure that all Employees complete their allocated training.

Conduct business only with approved counterparties

All Group entities will refuse to enter into, or continue, business with any counterparty who insists on anonymity or provides false, inconsistent or conflicting information where the inconsistency or conflict cannot be resolved after reasonable inquiry.

Reporting

All Employees should report any suspected violations of this Policy immediately by contacting the Compliance Department at compliance@arrowresources.com.

All reports will be kept in confidence to the extent appropriate, permitted by applicable law and consistent with the Group's policies. Any Employee that raises a concern in good faith will not be treated any differently or detrimentally, even if subsequent investigation does not support their concern. They will not be victimised or penalised for raising a concern.

Violations

Failure to comply with this Policy will be grounds for disciplinary action, including termination of employment.

Version History

Date:	Version:	Issued by:	Description:
16.11.2021	1.0	Compliance	v 1.0 issued

This Know Your Customer Policy has been approved by the Group's Board of Directors