



ELSEWEDY ELECTRIC

Group Anti-Money Laundering &
Counter Terrorism Financing

“AML&CTF” policy

V.2

2025

A large, white, curved line that starts from the left edge of the page and curves upwards and to the right, ending near the bottom right corner.

Table of Contents

1 INTRODUCTION	3
1.2 Policy Statement	3
1.3 Policy Objective	3
1.4 Scope	3
2 DEFINITIONS	3
2.1 Money Laundering	3
2.2 Terrorist Financing	4
2.3 Due Diligence ('DD')	4
2.4 Third Party	4
2.5 Persons with Significant Control	4
3 POLICY REQUIREMENTS	4
3.1 Due Diligence	4
3.2 Enhanced Due Diligence ('EDD')	5
3.3 Source of Funds	5
3.4 Payment Controls	5
3.5 Risk Assessment	5
3.6 Reporting and Escalation	6
3.7 Recordkeeping	6
4 ROLES AND RESPONSIBILITIES	6
4.1 All Covered Persons	6
4.2 Group Compliance	6
5 ANNUAL ATTESTATION	6
6 POLICY OWNER	6
7 POLICY REVIEW	6
8 VERSION CONTROL	7

1 INTRODUCTION

The Group Anti-Money Laundering and Counter Terrorism Financing Policy ('the Policy') of ELSEWEDY ELECTRIC Group ('EE') outlines our commitment to conducting business operations in compliance with Anti-Money Laundering and Counter-Terrorist Financing ('AML/CTF') laws and regulations wherever we operate. The Policy emphasizes our dedication to adhering to all applicable legal requirements, conducting our business in accordance with the highest standards, and promoting ethical business practices.

This policy should be read in conjunction with:

- EE's Sanctions Policy;
- EE's Whistleblowing Policy;
- The Employee Code of Conduct; and
- The Third-Party Code of Conduct.

1.2 Policy Statement

EE is committed to conducting all business activities with honesty, integrity, and the highest ethical standards. EE will not permit its products, services, or employees to be used to launder money or finance terrorism.

As an organization with global presence and operations, EE commits to complying with all applicable laws and regulations, in addition to international recommendations such as the Financial Action Task Force (FATF).

Violations of this policy will result in disciplinary action, including dismissal and financial penalties, and may lead to prosecution under applicable local and international laws.

1.3 Policy Objective

The purpose of this Policy is to:

- Define EE's commitment to ethical conduct, and compliance with applicable laws and international best practices.
- Protect EE, its employees, and stakeholders from the legal, financial and reputational risks associated with Money Laundering and Terrorist Financing.
- Ensure consistency in the application of AML/ATF measures across EE.

1.4 Scope

This Policy applies all EE operations worldwide, all EE subsidiaries, and to every EE employee, agent, contractor, consultant, distributor, supplier or joint venture partner working with the EE or on its behalf ('Covered Persons').

Whilst this policy represents the minimum procedural requirements, a more restrictive approach can be adopted by local EE subsidiaries where necessary to comply with local laws. In case of conflict between this policy and local legislation, the matter must be submitted to Group Compliance.

2 DEFINITIONS

2.1 Money Laundering

Money laundering is used to conceal the source of funds gained through illegal activities, such as (but not limited to) fraud, corruption, tax evasion, drug or human trafficking.

Money laundering consists of three stages:

- Placement: where illegal funds are deposited into the financial system, (**e.g.**, paying for goods in cash).
- Layering: consists of confounding the trail of the illegal funds to disguise its source and/or ownership.
- Integration: Integrates the funds into the economy to make it appear legitimate.

2.2 Terrorist Financing

Terrorist financing consists of providing financial support to individuals or groups engaged in terrorism.

2.3 Due Diligence ('DD')

The process of thoroughly investigating and evaluating an organization/individual to ensure it adheres to all applicable laws, regulations, and industry standards.

2.4 Third Party

For the purpose of this policy, third party includes any counter party transacting with EE, **e.g.**, customer, supplier, service provider, intermediaries, subcontractor, individuals or corporates.

2.5 Persons with Significant Control

A person with significant control is an individual who:

- Owns 25% or more of the shares or voting rights in a company;
- Has the right to appoint or remove the majority of the board of directors; or
- Exercises significant influence or control over the company.

3 POLICY REQUIREMENTS

3.1 Due Diligence¹

Prior to establishing a business relationship with any third party, all Covered Persons must:

- Complete a Due Diligence Questionnaire ('DDQ'), the business owner of the relationship must ensure the DDQ has been completed and shared with Group Compliance prior any official engagements (e.g., Contract, Purchase Order...);
- Obtain identification documents in accordance with the checklist in the Due Diligence Procedure;
- Submit the DDQ and identification documents to Group Compliance;
- Once Group Compliance have the above documentation, it will conduct a risk assessment in line with the Customer Risk to Control Library ('CRTCL') maintained by Group Compliance and consider what further information or documentation is required;
- **No Covered Person may proceed** with the business relationship, sign any contract, or execute any transaction until Group Compliance has reviewed the DDQ, identification documents, conducted the risk assessment, and confirmed it may proceed.

For ongoing business relationships, all Covered Persons must keep the relationship under review, and immediately report any red flags to Group Compliance.

¹ Refer to the Group Due Diligence Procedure.

3.2 Enhanced Due Diligence ('EDD')

For high-risk third parties, high-risk transactions, or transactions involving high risk jurisdictions as identified in the initial due diligence process, Group Compliance will advise on **EDD** measures. Group Compliance will specify what EDD is required, but it will usually include:

- Certified copies of DD documents;
- Documentary support for source of funds information;
- Initial and periodic verification of public source information to confirm DD information;
- Raising any discrepancy between the explanation for source of funds and source of wealth and information in the public domain with Group Compliance;
- Ongoing monitoring.

3.3 Source of Funds

Before receiving funds from a newly contracted third party, entering into a new contract a third party, or in relation to any high-risk or complex transaction, the source of those funds must be obtained and provided to Group Compliance. Source of funds refers to the origin of the money being used in a transaction and should show what that is. Acceptable documents include:

- Audited company accounts;
- Bank statements showing transaction history;
- Sale agreements (**e.g.**, property, shares);
- Loan agreements;
- Dividend or investment income records.

3.4 Payment Controls

- Covered Persons must not receive or make payments from or to any third party that is not contracted with EE;
- No payment will be processed if not aligned with the contractual payment terms **i.e.**, amounts, currency, bank account details.
- Any payment to third party must be made **only** to the third party's bank account that is evident in the DDQ and the Contractual agreement.
- Cash payments received from third parties should be minimal and on exceptional basis.
- No payments will be made to an offshore account or any jurisdiction not related to the business relationship or as contractually agreed with the third party.
- In case of any refunds **i.e.**, EE has been overpaid by a third party, must be pre-approved by the entity Chief Financial Officer and reported to Group Compliance.
- Any requests to change the contractually agreed payment terms, currencies, or bank account details, must be reviewed by Legal and Compliance and approved by the entity Chief Financial Officer.

3.5 Risk Assessment

- EE Group Compliance will conduct an enterprise-wide AML/CFT risk assessment at least annually or whenever there are significant changes (**e.g.**, entering new markets).
- The risk assessment methodology and outcomes will be documented and reviewed by senior management.
- Assessment outcomes and rating should inform the level of due diligence and control environment required.

3.6 Reporting and Escalation

Any Covered Person who suspects a violation of this policy must report their concerns immediately to Group Compliance compliance-int@elsewedy.com, or [the Speak Up² tool](#).

3.7 Recordkeeping

All counterparty Due Diligence reports, identification documents, source of funds documents, transaction details, and any other relevant records will be retained by Group Compliance for five years or as per the local legal requirement.

4 ROLES AND RESPONSIBILITIES

4.1 All Covered Persons

The responsibility for preventing, detecting, and reporting money laundering and terrorist financing rests with every member of EE. All Covered Persons must:

- Ensure that they have read and understand this policy.
- Comply with this policy and policies referred to therein at all times.
- Cooperate fully with internal audits, reviews, and investigations.

4.2 Group Compliance

Group Compliance is responsible for:

- Maintain accurate recordkeeping in respect of DD and source of funds.
- Review all DDQs, and any supporting documents in a timely manner.
- Suggest enhanced due diligence for high-risk third parties or transactions.
- Ensure mitigation controls are communicated with the business relationship owner for implementation.
- Ensure all Covered Persons receive appropriate AML/ATF training.
- Conduct annual AML/ATF risk assessments for EE.

5 ANNUAL ATTESTATION

All employees will be required to attest upon joining the group and then annually, that they have read, understood, and will observe the requirements of our Code of Conduct and compliance policies.

6 POLICY OWNER

Group Compliance is the owner of this policy.

Questions and feedback regarding this policy must be submitted to Group Compliance: compliance-int@elsewedy.com

7 POLICY REVIEW

This policy shall be reviewed annually and/or when deemed necessary.

² Refer to Group Whistleblowing Policy.

8 VERSION CONTROL

Title of document	Group Anti-Money Laundering and Counter Terrorism Financing “AML & CTF”		
Version no.	V.1.1	7/Mar/2024	Minor amendments
	V.1.2	28/Nov/2024	Minor amendments
	V.2	07/Dec/2025	<ul style="list-style-type: none"> - Template Update - Further elaboration on source of funds & payments controls. - Included a reference to Risk Assessment.
Document Drafted by	Group Compliance		
Document approved by	Group CEO and Group CLCO		
Date of next review	December 2026		