ELSEWEDY ELECTRIC

Fraud Control Policy

V.2

2026

Table of Contents

1 INTRODUCTION

Elsewedy Electric Group ('**EE**', the '**Group**') is committed to maintaining the highest standards of integrity, transparency, and accountability in all of its operations.

Fraud undermine trust, damage reputation, and pose serious legal and financial risks to our Group, our employees, and the stakeholders we serve.

This Fraud Policy, (the '**Policy'**) outlines El Sewedy Electric establishes a framework for preventing, detecting, and responding to fraudulent activities.

1.1 Policy Statement

EE is committed to conducting its business with honesty, integrity, and the highest ethical standards. We take Zero-tolerance approach to fraudulent activities.

This commitment extends to all our activities, in every country we operate, and involves all individuals working with or on behalf of EE and any of its subsidiaries.

Fraud refers to all acts of: fraud, breach of trust, misappropriation, wasting, embezzlement, bribery, causing harm to, and what is deemed as public property also every illegal act that could affect the public financial interest for the Group.

For the purpose of this policy, fraud, misconduct and corruption will be encompassed into the word "Fraud" (hereafter 'Fraud').

1.2 Policy Objective and Scope

The Policy is designed to ensure the following:

- **Define the responsibilities** of EE and all entities/individuals working on its behalf in upholding the Group's zero-tolerance stance on Fraudulent activities.
- **Provide clear guidance and practical information** to employees and business partners on how to identify, prevent, and respond to suspected or actual instances of Fraud.
- **Ensure consistency** in the application of Fraud prevention controls across EE.

1.3 Scope

This Policy applies to 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. POLICY REQUIREMENTS

2.1 Prohibited Conduct

The following actions constitute fraud and are strictly prohibited under this policy:

- Misappropriation, theft, or unauthorized use of organizational funds, assets, or property;
- Falsification, alteration, or destruction of financial records, reports, or supporting documentation;
- Submission of false or inflated expense claims, invoices, or procurement requests;
- Bribery, kickbacks, or any for of corrupt payment to or from third parties;
- Unauthorized disclosure or misuse of confidential or proprietary information for personal gain;
- Identify fraud, impersonation, or misrepresentation in any business transaction;
- Collusion with external parties to defraud the organization or its customers.

3. FRAUD PREVENTION AND INTERNAL CONTROLS

Management must adopt a preventative approach for identifying, analyzing and managing the risk of Fraud that could prevent the Group from achieving its business objectives or strategies.

3.1 Fraud Risk Assessment

A Fraud Risk Assessment shall be performed on a systematic and recurring basis, involve appropriate personnel, consider relevant Fraud schemes and scenarios, and map those Fraud schemes and scenarios to mitigating controls.

3.2 Fraud Prevention Controls

3.2.1. Affirmation Process (Declaration)

All the Group Employees and Stakeholders shall acknowledge they have read, understood, and complied with the Fraud Control Policy to support the This shall be submitted electronically or via manual signature. The Group will apply disciplinary action for refusal to sign-off and apply such action consistently. See Appendix C Acknowledgement Form.

3.2.2. Disclosure of Conflict of Interest

All employees and stakeholders must disclose potential or actual conflicts of interest if they are responsible for covering out any procedure or taking a decision or express an opinion. The management has to be informed through the employee immediate superior.

This should be documented according to the requirement of the Code of Conduct. Any constraints placed on the situation must be monitored.

3.2.3. Human Resources Procedures

The Human Resources Department (HR) shall:

- Perform background investigations, document verification process to verify match skills to the job requirements, and be aware of any issues of personal integrity that may impact on their suitability for the position.
- Confirmation of work history and education presented on a job application or résumé.
- Evaluation performance and compensation programs of all Group employees must take into consideration work related competence, the behavior and performance as per this Policy.
- Conduct exit interviews of terminated employees or those who have resigned. HR must review the content and information contained in resignation letters as they may contain information regarding possible Fraud existing within the Group.

3.2.4. Authority Limits

The Board must establish authority approval levels across the enterprise to serve as an entity-level control. Individuals working within a specific function must be assigned only limited IT access as a process-level control.

4. FRAUD DETECTION

4.1. Fraud Detection Procedures

- The Group must have effective automated systems to identify potential red flags within the financial transactions. The Group shall use data analysis, continuous auditing techniques, and other technology tools effectively to detect Fraud activity.
- Continuous auditing must be conducted with the use of data analytics on a continuous or real-time basis, thereby allowing management or auditing to identify and report Fraud effectively. The Group employees shall ensure the greatest possible transparency of transactions to have effective controls of defense against Fraud. These systematic approaches that assist in detection and prevention involve both internal and external processes.
- The Group should have a reporting mechanism in place that provides for anonymity, unless the employee reporting the fraud case expressed his desire to disclose his name, to any individual who willingly comes forward to report suspicious fraud and encourages such reporting. The Group preserves the confidentiality of the reporter during the investigation process and provides assurance to employees that they will not be retaliated against for reporting their suspicious of wrongdoing including wrongdoing by their superiors.

5. FRAUD REPORTING PROCESS

- The Group employees shall inform their direct superiors or the higher management of any suspected Fraud activities that comes to their attention. If the instance is related to the employee direct superior or any senior employee in the Group, the employee may report the case to the legal or compliance department or via the whistleblowing tool[1].
- The immediate superior or the higher management shall inform the Legal Department about the case when it comes to their attention to take the necessary action and decide on the required Internal Audit procedures, conducting investigations or informing the concerned supervisory and law enforcement bodies to take the necessary action.

6. INVESTIGATION PROCESS

The Group must conduct the investigation of the Fraud cases related to the employees according to any disciplinary policy applied to the Group.

The Investigator or the Investigation Committee may hear the statement of the complainant or inform and collect evidence under the supervision of the Legal Advisor. The Legal Advisor can do all or some of the above mentioned for the purpose of making it available.

The investigation plan should include the following procedure:

- Confidentiality: Information gathered must be kept confidential and distribution limited to those who have a legitimate need to know. This is important to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Group from potential civil liability.
- Legal Involvement: Legal counsel must be involved early in the process or, in some cases, in leading the investigation, will help safeguard work product and attorney-client communications.

[1] Please refer to Group Whistleblowing Policy.

- Securing evidence: Evidence must be protected so that it is not destroyed and so that it is admissible in legal proceedings.
- Notification notifying the concerned parties, law enforcement, and regulators with the outcome of the investigations (as applicable).

6.1. Reporting the Results

The investigation team shall report its findings to the party overseeing the investigation, such as Management and/or legal counsel.

6.2. Corrective Actions

After the investigation has been completed, the Group must determine follow up actions. The Group shall consider the potential impact of its response and the message that it may send to the public, stakeholders, and others.

6.3. Recovery of the proceeds of Fraudulent Conduct

The Group shall take all reasonable steps, including the institution of criminal or civil proceedings to recover property of the Group that has been misappropriated or otherwise been obtained as a result, either directly or indirectly of Fraud.

7. ROLES AND RESPONSIBILITIES

All covered persons share responsibility for upholding the Group standards. Specifically:

- Employees and Contractors: Required to act with honesty and integrity at all times, refrain from engaging in or facilitating fraudulent activity, and report any known or suspected fraud promptly.
- Managers and Supervisors: Responsible for promoting a culture of ethical conduct within their teams, ensuring staff are aware of and trained on this policy, escalating concerns or allegations in a timely manner.
- Senior Leadership and the Board: Responsible for setting the tone at the top, ensuring adequate resources are allocated to fraud prevention and detection, and overseeing the organization's overall fraud risk management framework.
- Finance and Internal Audit: Responsible for implementing and monitoring internal controls, conducting periodic risk assessments, and leading or supporting fraud investigations as required by Group Compliance.

8. REVIEW OF FRAUD CONTROL ARRANGEMENTS

This Policy shall be reviewed by the Board, on recommendations from the Audit Committee and updated on a regular basis.

9. 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

10. POLICY REVIEW

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

11. VERSION CONTROL

Title of document	Fraud Control		
Version Control	V.1	November 2024	- Policy Drafted
	V.2	December 2025	- Update to roles and responsibilities section. - Update the Objectives, Statement, and Scope to align with the Group Compliance policies.
Document Drafted by	Group Compliance		
Document approved by	Group CEO and Group CLCO		
Date of next review	December 2026		