MOBILE TELECOMMUNICATIONS COMPANY (ZAIN)

SANCTIONS POLICY

FEBRUARY 2026

Documentation Authorization Control Sheet

Document Type	Policy
Custodian	Corporate Governance
Version	1.2

Version	Date	Author	Approved By	Comments
1	2020	CG	Board of Directors	Establish policy
1.2	2026	CG	Board of Directors	**Updated based on the separation of roles of the Governance & Compliance departments**

Contents

Glossary

Term	Definition
The Company	Mobile Telecommunications Company K.S.C.P. (Zain Group) (Zain) and all its subsidiaries
The" Board"	Board of Directors (BOD) of Zain Group
The Policy	The approved Sanctions Policy of Zain Group
Executive Management	CEO, C-level management and any other member with a direct reporting line to the CEO.
CG Dept	Corporate Governance and Compliance department
Employees	All employees at the company at all levels.
Business Units	Operating company subsidiaries in each market and group departments at the Company representing a specific business function
Sanctions Laws and Regulations	Any economic, sectoral, financial or trade sanctions laws, regulations, restrictions adopted, administered, enacted or enforced by any Sanctions Authority; or any other relevant law, enabling legislation, executive order or regulation.
Sanctions Authority	Any authority of (a) the United States of America (including its Office of Foreign Assets Control (OFAC); (b) the United Nations; (c) the European Union or an individual member state thereof; or (d) the United Kingdom. (e) any other authority as deemed necessary for the Company's business operations
CTF	Countering terrorist financing
AML	Anti-Money Laundering
Sanctions List	any published list of persons adopted under Sanctions Laws and Regulations made by any Sanctions Authority from time to time.
Sanctioned Person	any person or entity that is: (a) listed or referred to on any Sanctions List;

Term	Definition
	(b) resident, located or operating in, or incorporated under, the laws of any country or territory that is the target of the comprehensive, country- or territory-wide Sanctions; and/or (c) that is otherwise a target of Sanctions Laws and Regulations.
Suppliers	All suppliers of goods or services to the Company

1. Introduction

Zain Group has developed this Policy in line with the applicable Sanctions Laws and Regulations.

This Policy summarizes preventive actions imposed by Sanctions Authorities which control the ability of the Company to undertake any activity in certain high-risk territories or with Sanctioned Persons.

This Policy also outlines the restrictions and protective measures to be consistently followed by each Employee of the Company. The Company is committed to complying with Sanctions Laws and Regulations in all jurisdictions of its operations.

2. Purpose

The purpose of this Policy is to provide guidance on how to comply with applicable Sanctions Laws and Regulations. This Policy sets the high-level principles and standards of management of financial crime risks for Zain, including money laundering, terrorist financing and sanctions breaches, and constitutes a part of the Board of Directors' Instructions to the Executive Management.

The objective of this Policy is to ensure regulatory compliance and to establish an internal framework that minimizes the risk of sanctions breaches and abuse of the Company's products and services for money laundering and terrorist financing purposes. This is in alignment with the Company's strategy, which sets the Company's vision to be recognized as the most trusted network provider.

This Policy covers the implications associated with non-compliance with the Sanctions Laws and Regulations, as well as the reporting process of such violations.

3. Scope and Application

The Policy applies to all Employees and persons in a comparable position, all functions, all Business Units within Zain Group, and all subsidiaries, once adopted by their Executive Management.

In the event that this Policy conflicts with local legal requirements, Executive

Management may approve deviations from this Policy but the same must be reported to the Board of Directors.

The aim of the Company is not only to comply with relevant legal requirements but also to mitigate and reduce the potential financial and public relations risk to the Company of our Suppliers and Customers using transactions with Zain Group to launder the proceeds of illegal activity, fund terrorist activity or breach financial sanctions.

The Company must comply with the relevant laws and regulations in which it operates and may, based on its risk tolerance, adopt more exacting standards than those set out in this Policy.

4. Confidentiality

The contents of this Policy are confidential and are intended for internal use only.

The Policy should always be kept in a safe place and must not be copied or disclosed to third parties (i.e. persons not employed by the Company) without the express written permission of the Executive Management.

5. The Company's measures towards money laundering/terrorist financing and financial sanctions

The Company is undertaking a number of initiatives to strengthen its ability to ensure its compliance with the requirements outlined in this Policy. The Company will, therefore, continually assess its existing policies, procedures, controls and IT systems and make necessary changes to be most effective in accordance with the risk-based approach.

6. Obligations

- Through this Policy, the Board of Directors has instructed the Executive Management to implement a robust approach within the Company to seek to prevent money laundering, terrorist financing and breaches of financial sanctions. It is the responsibility of the Executive Management in coordination with the Compliance Department, to ensure that the Company complies with the measures outlined in this Policy.
- The Business Units, as the first line of defense, are accountable for the risks related to financial crime.
- Compliance Department and Risk Management, as the second line of defense,

are responsible for identifying, monitoring, assessment, guidance and reporting of money laundering, terrorist financing and financial sanctions risks. and understanding the ML/TF risks to which the Group is exposed and to take measures to those risks for the purpose of mitigating them effectively.

- Internal Audit – is responsible for carrying out independent testing of the Company's policies, procedures and controls.
- The Company maintains this Policy to meet its requirements of business operations under relevant authorities.
- The Company will use all reasonable endeavors to ensure that its business and transactions do not involve a breach of any applicable Sanctions Laws and Regulations.
- The Company will use all reasonable endeavors to check relevant third parties (such as Suppliers) against Sanctions Lists to reduce the risk of transacting with Sanctioned Persons.
- The Company will use all reasonable endeavors to check Customers (natural persons or companies) against Sanctions Lists so as to reduce the risk of transacting with Sanctioned Persons.
- Employees must be regularly informed about the updates in the Company's Sanctions Policy and relevant Laws and Regulations.
- Employees must report about any breaches or potential breaches of applicable Sanctions Policy and Laws and Regulations.
- In case of conflict between the above-mentioned principles and any business requirements, these principles shall prevail.

7. Group-wide Operations

The Company operates in several market areas with a range of financial products being offered to multiple customer segments. Accordingly, the Executive Management intends to establish an overall group-wide requirements and standards for financial crime in order for all OpCos to comply with.

8. FinTech

In parallel to the verification of the identity of Customers of the Company's financial services products, the Company intends to apply a risk-based approach towards the collection, registration, and monitoring of information in relation to the nature and intent of the customer relationship.

The Company will include in its terms and conditions with Customers of its financial services products a right for the Company to suspend or terminate accounts in the event of the relevant Customer appears on the sanctions lists or watchlists issued by the regulators of financial services in the countries where the Company operates.

Given the volume of Customer/ Supplier, the Company has an effective initial registration and ongoing monitoring of the Company's database. It is essential that natural persons and legal entities are identified and screened.

The Company undertakes significant effort to determine the ownership and control structure of legal entities. Therefore, the Company must identify and verify the identity of any natural persons who ultimately owns or controls the Suppliers to the Company.

9. Screening of politically exposed persons

In order to ensure that natural persons defined as politically exposed persons ("PEPs") are identified and registered in the Company's system as such, a PEP screening process will be conducted after natural persons have been on-boarded. Furthermore, the database will be screened for PEPs on an ongoing basis.

10. IT Systems

The Company's IT solution must be designed to ensure that robust internal controls of Customer/Supplier due diligence are maintained.

This requires strong data quality and, where possible, automatic ongoing due diligence between public registries and the Company's IT systems. Data quality shall be measured and reported as a key performance indicator.

11. Transaction monitoring

Transaction monitoring shall, based on a risk-based approach, cover all Business Units, all Customers, all Suppliers and all market areas, once a complaint is made or suspicious transactions/behaviors are detected. The manual transaction monitoring – investigating and reporting of the unusual activity to the Compliance Department, Risk Management, and Internal Audit - is achieved through training and awareness campaigns.

12. Sanctions Screening

In order to comply with the Sanctions Laws and Regulations, relevant control procedures must be in place.

The Company plans to implement a screening solution, as part of the Company's overall strategy to ensure that the Company is compliant with the applicable AML, CTF and financial sanctions regulations.

13. Retention and record-keeping

For the purpose of preventing, detecting and investigating unusual and suspicious transactions, the Company must keep electronic records of all transactions and due diligence measures carried out in accordance with this Policy.

Records must be kept in a manner making information and documents available to all Employees having appropriate access (within the Company's existing IT solution).

Documentation must be kept during the lifetime of the relevant entity's relationship with the Company according to the applicable laws, regulations and standards. Such documents shall be maintained at least five years after termination of the relationship or after the date of an occasional transaction.

14. Training and awareness

The Company requires that all Employees possess an adequate awareness level of the risks of financial crime. The Company must ensure that all Employees have a suitable degree of awareness, i.e. when staff become aware of unusual or suspicious transactions, they must consider whether this may be related to ML, TF and/or sanction evasion.

15. Escalation and Reporting

The Company has an escalation process stating the requirements for appropriate and timely internal reporting of potentially problematic cases across Zain Group. The requirements in the escalation process must always be considered in relation to the violation of the Company's obligations to prevent and mitigate financial crime with adherence to other related policies and governing documents.

16. Review

This Policy must be reviewed by Corporate Compliance Department to ensure alignment with emerging laws and regulations or however needed. Any changes to the Policy must be endorsed by the Corporate Governance Department and approved by the Board of Directors.

17. Non-Compliance

In case any Employee breaches any applicable Sanctions Laws and Regulations or the Company's Sanctions Policy, the Executive Management, shall consult with the Head of the Concerned Department, the Risk Management Department, the Human Resources Department and Corporate Compliance Department, to immediately take corrective actions in accordance with applicable labor laws and regulations.

In case the Company breaches Sanctions Laws and Regulations or the articles of this policy due to changes in the Sanctions Laws and Regulations, the Executive Management shall immediately report to the Group Legal, Risk Management and CG departments.

The Company shall seek to include in its terms and conditions with Suppliers an obligation to comply with Sanctions Laws and Regulations and a right for the Company to terminate the agreement in the event of a breach of the same. The Company shall also take all necessary measures to address such breaches, such as suspending and/or terminating relevant contracts to ensure that there is no violation of applicable Sanctions Laws and Regulations.