AMBUJA CEMENTS LIMITED

Sanctions Compliance Policy

(Adopted on 30th January 2026)

TABLE OF CONTENTS

Sr. No.	Particulars	Page Nos.
1.	Policy Statement	3
2.	Scope	3
3.	Purpose	3
4.	Sanctions Overview	4
5.	Requirements 5.1. Red Flags 5.2. Transactional Due Diligence Requirements 5.3. Vessel and Port Due Diligence 5.4. Recordkeeping 5.5. Training 5.6. Duty to Report and Cooperate	6
6.	Disciplinary Measures	10
7.	Anti-Retaliation	10
	Appendix A: Red Flags	11
	Appendix B: Transaction Due Diligence Checklist	13

1. Policy Statement

The Adani Group and its various subsidiaries (each individually the "**Company**" or together the "**Companies**") seek to conduct business in compliance with sanctions laws and regulations of the United Nations ("**UN**"), the European Union ("**EU**"), the United States of America ("**U.S.**"), and the United Kingdom ("**UK**") (collectively, "**Relevant Jurisdictions**") (collectively, "**Sanctions Laws**").

No business *interest justifies a breach of Sanctions Laws.*

2. Scope

This Sanctions Compliance Policy (the "**Policy**") applies to all directors, officers, and employees of the Companies, including all individuals employed by any entity owned and/or controlled by the Companies ("**Employees**"). The Policy also applies to contractors, consultants, suppliers, vendors, agents and any other persons working under the Company's supervision or direction ("**Contractors**" and collectively with Employees, "**Company Personnel**"), which the Companies shall establish in applicable agreements, including but not limited to the Companies' Supplier Code of Conduct.

3. Purpose

The purpose of this Policy is to set out the core requirements of sanctions compliance with respect to the business activities of the Companies. The Policy establishes protocols for complying with the Sanctions Laws and identifies best practices for mitigating associated risks.

This Policy provides requirements and guidance to facilitate compliance with Sanctions Laws, but it is not intended to indicate whether any particular transaction is permitted. It shall be read in conjunction with the applicable laws, regulations, orders and guidance issued from time to time by the Relevant Jurisdictions, as well as any advisories, standard operating procedures, and other protocols issued from time to time by the Companies or the Adani Group.

Any questions concerning this Policy or any perceived conflict with its requirements shall promptly be referred to the Head of Compliance.

4. Sanctions Overview

Sanctions are economic, financial, and trade restrictions on, or on transactions with or involving, certain countries, governments, entities, individuals or sectors. They may affect commercial dealings with sanctioned counterparties by prohibiting unlicensed trade (e.g., export/import control restrictions), imposing asset freezes, prohibiting certain types of unlicensed commercial and financial transactions (including payment processing), or a combination of these measures.

Sanctions may be comprehensive (meaning they apply to any party organized or located in a jurisdiction) or targeted/list-based.

Importantly, sanctions may extend beyond persons directly designated by a sanctioning jurisdiction, such as the U.S., UK, and EU. Sanctions may extend to entities owned or controlled by directly designated persons. The precise approach to ownership and control depends on the

Relevant Jurisdiction. For example, the U.S. generally applies a 50% ownership test, whereas the EU and the UK apply additional complex control tests. If you need guidance on whether a person should be regarded as owned or controlled by a directly designated person, you should consult with the Head of Compliance.

Generally, sanctions apply whenever there is a connection (a so-called "nexus") to the sanctioning jurisdiction, such as the U.S., UK, or EU. A nexus most obviously arises where a party involved in a transaction is a national of, conducts business in, is resident in, or is incorporated or registered in the sanctioning jurisdiction.

UK sanctions are extended to all British Overseas Territories (except Bermuda and Gibraltar). For example, companies incorporated in the British Virgin Islands or the Cayman Islands are covered by UK sanctions.

In the case of U.S. sanctions, the use of U.S. dollars in a transaction also establishes a sufficient nexus, even if the parties have no other connection to the U.S.

The U.S. sanctions regime imposes a strict liability standard. This means that a party may be penalized for sanctions violations even when the party did not intend to engage in prohibited conduct and even if a compliance policy or procedure meant to prevent such violations was in place.

The global shipping industry is an area of particular sanctions risk. Relevant Jurisdictions have sanctioned a broad range of actors in the shipping industry, including maritime insurance companies, charterers, vessels, suppliers of cargo, customs and port state controls, flag registries, ship owners, shipyards, and financial institutions involved in maritime trade finance. The latest guidance on Sanctions Laws by the UN, EU, UK and U.S. are available on respective websites and should be referred. Further updated guidance may be circulated by the Compliance department from time to time. Notwithstanding the same, the Company Personnel whose roles relate to shipping shall review up-to-date guidance issued by relevant authorities at the time of such issuance. Sanctions designations change frequently. Company Personnel shall undertake real-time diligence efforts, described below, to ensure that any potential counterparty, vessel or cargo is not sanctioned.

All Company Personnel shall comply with all Sanctions Laws.

4.1 Comprehensive Sanctions

Comprehensive sanctions are sanctions imposed on countries or regions as a whole and generally *prohibit all dealings or transactions with any party organized or located in the sanctioned country or region, the government (including any political subdivision, agency, or instrumentality) of that country or region, or involving goods from that country or region.*

As of the date of this Policy, countries/regions under comprehensive sanctions include the Crimea, so-called Donetsk People's Republic and Luhansk People's Republic regions of Ukraine, Cuba, Iran, and North Korea.

Transactions of any form with or involving comprehensively sanctioned countries or regions are strictly prohibited.

4.2 List-Based Sanctions

List-based sanctions prohibit certain transactions or other dealings with or for the benefit of parties identified on one or more lists maintained by the Relevant Jurisdictions ("**Sanctions Lists**"), such as:

- The U.S. Consolidated Screening List.[1]
- The UN Security Council Consolidated List.[2]
- The EU Sanctions Tracker[3] and Consolidated List of Designated Vessels.[4]
- The UK Sanctions List and the OFSI Consolidated List Search.[5]

The prohibitions with respect to parties identified on one or more Sanctions Lists may be broad in nature, such as a prohibition on dealing with such party or in any property in which such party has an interest, or may be narrower in scope, such as a prohibition on the acquisition of equity interests or debt issued by such party. Company Personnel who need guidance on the nature of the prohibition/(s) with respect to parties identified under Sanctions Lists shall consult with the Head of Compliance.

Company Personnel shall not engage in any activities with or involving any party identified on a Sanctions List.

5. Requirements

The steps required to prevent sanctions violations and mitigate sanctions risk depend on the nature of the parties and transactions. Company Personnel shall consider these factors when determining which measures identified below to employ. In the case of uncertainty, Company Personnel shall seek guidance from their supervisor or the Head of Compliance.

5.1 Red Flags

Red flags are indicators that a transaction or business relationship might involve an attempt to evade sanctions. A red flag is not always indicative of sanctions evasion, but it is an indicator that Company Personnel should undertake additional due diligence before moving forward with a transaction.

Appendix A contains a non-exhaustive list of red flags to which Company Personnel should be alert. If one or more red flags are observed, Company Personnel shall escalate the issue to their supervisor or the Head of Compliance before proceeding with the transaction. The manner in which red flags are identified, escalated, and resolved will necessarily vary by business unit.

---

[1] https://www.trade.gov/consolidated-screening-list. This screening list consolidates Sanctions Lists administered by the Department of the Treasury's Office of Foreign Asset Controls ("OFAC"), the U.S. Department of State and the U.S. Department of Commerce.
[2] https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list
[3] https://data.europa.eu/apps/eusanctionstracker/
[4] *Link available* at https://www.sanctionsmap.eu/#/main
[5] https://search-uk-sanctions-list.service.gov.uk/

5.2 Transactional Due Diligence Requirements

The Companies are responsible for ensuring that they do not transact with or for the benefit of sanctioned parties or otherwise in violation of Sanctions Laws. Prior to engaging in a transaction in which a Company is a party, Company Personnel shall undertake the following procedures ("**Due Diligence**") with respect to each potential counterparty:

- Require the potential counterparty to complete the Know Your Customer ("**KYC**") Questionnaire, including providing relevant documents, as per the Companies procedures. including requirement to obtain a country-of-origin certificate to mitigate risks related to US/EU sanctions.
- Search for the potential counterparty's name, as well as the name(s) of any individual or entity having 20% or more direct or indirect ownership in the potential counterparty, on the U.S. Consolidated Screening List[6], the UK Sanctions list and the OFSI Consolidated List Search,[7] the EU Sanctions Tracker and Consolidated List of Designated Vessels[8] and the UN sanctions list[9] (collectively, a "**Sanctions Screen**").
- Conduct open-source research on the potential counterparty to identify any red flags.

A Sanctions Screen shall be conducted for each transaction, and for each counterparty involved in the transaction, regardless of whether the counterparty is familiar to the relevant Company and has previously been subject to Due Diligence.

Company Personnel may rely on verified documents provided by counterparties unless red flags are present. If red flags are present, the transaction shall be suspended while the issue is escalated to a supervisor or the Head of Compliance, who, in consultation with other Company Personnel as appropriate, shall take necessary steps to look into and resolve the red flags.

The Companies shall include in all contracts adequate controls/ clauses including, as appropriate, rights to due diligence documents, warranties regarding compliance with the Sanctions Laws, and termination and indemnification rights in the event of a sanctions violation by the counterparty.

5.3 Vessel and Port Due Diligence

Company ports shall not provide any services to or for any vessel that is itself sanctioned or that is owned or managed *by or for the benefit of a sanctioned entity or person, or facilitate shipment of sanctioned goods or by or for the benefit of a sanctioned entity or person.*

Company Personnel engaged in transactions involving vessels or import/export shipments shall:

- Run a Sanctions Screen on the vessel name
- Verify that the vessel is not flagged in a sanctioned country
- Run a Sanctions Screen on the vessel's operator/manager
- Run a Sanctions Screen on the vessel's owners (up to the ultimate beneficial owner)
- Verify the last ten ports of call via a reliable third-party intelligence system database to ensure that the vessel has not visited sanctioned ports or spent undue time in

[6] Consolidated Screening List
[7] UK Sanctions List and OFSI Consolidated List Search
[8] EU Sanctions Tracker and EU Sanctions Map
[9] UN Sanctions List

sanctioned waters.

Company Personnel may rely on verified documents provided by counterparties unless red flags are present. If red flags are present, the transaction shall be suspended while the issue is escalated to a supervisor or the Head of Compliance, who, in consultation with other Company Personnel as appropriate, shall take necessary steps to look into and resolve the red flags.

If any of these steps cannot be completed or result in a sanctions concern, Company Personnel shall escalate the issue to their supervisor or the Head of Compliance.

5.4 Recordkeeping

A **Transaction Due Diligence Checklist**, available at **Appendix B**, shall be completed for each potential transaction. This Checklist shall be saved in a shared network location that is easily searchable and auditable, along with all documents received as part of the Due Diligence process, including but not limited to contracts, invoices, and certifications (the "**Transaction File**"). These records shall be maintained for 10 years.

5.5 Training

The Companies shall provide annual training to promote awareness of the Companies' obligations under the sanctions laws and to help Company Personnel understand their roles and responsibilities under this Policy. All designated Company Personnel are required to participate in and complete the general sanctions training program. The Companies will also provide job-specific sanctions training on an as-needed basis. The Companies will track and maintain records of the participation of Company Personnel in the sanctions training program, and will maintain these records for 10 years

5.6 Duty to Report and Cooperate

Company Personnel who become aware of an actual or potential violation of this Policy or any Sanctions Law shall, as soon as practicable, contact their supervisor, the Legal Department, or the Head of Compliance. If that contact is verbal, the Company Personnel shall subsequently create a written record describing the issue and resolution, which will be saved in a shared location on the relevant Company's computer network.

The Companies expect and require that all Company Personnel will fully cooperate with the Legal and Audit Departments of the Companies, outside counsel and auditors, or other similar parties engaged by the Companies in any audits, investigations, and inquiries related to this Policy.

5.7 Audit

The Companies shall conduct audits in the ordinary course to ensure adherence to their obligations under applicable Sanctions Laws.

6. Disciplinary Measures

The Companies do not tolerate direct or indirect violation of sanctions. Nor will the Companies tolerate failure to adhere in good faith and with best efforts to the requirements of this Policy.

The Companies reserve the right to take disciplinary measures, up to and including termination of employment or contractual relationships, for any non-compliance with this Policy.

7. Anti-Retaliation

The Companies will not criticize any loss of business resulting from adherence to this Policy. Company Personnel will not be penalized or suffer adverse employment decisions for bringing to the attention of management, in good faith, a known or suspected breach of this Policy or any Sanctions Law. Refer to the relevant Company's Whistleblower Policy for additional information.

****

APPENDIX A: Red Flags

Company Personnel shall remain alert to any indicia of sanctions violations or attempts to circumvent Sanctions Laws. Signs that a counterparty may be attempting to circumvent Sanctions Laws are known as red flags. If one or more red flags is observed, Company Personnel must escalate the issue to their supervisor or the Head of Compliance before proceeding with the transaction. Presence of a red flag does not prohibit the contemplated transaction, but rather means only that an additional level of diligence is required. **The examples listed below are not exhaustive.**

General Red Flags

- The counterparty or its beneficial owner is listed on any Sanctions List.
- The counterparty is incorporated or domiciled in a jurisdiction subject to either comprehensive sanctions such as Crimea, the so-called Donetsk People's Republic and Luhansk People's Republic regions of Ukraine, Cuba, Iran, and North Korea, or sector-specific sanctions regimes, including but not limited to Russia, Venezuela, Belarus, and Yemen.
- The counterparty has a name or address similar to a sanctioned entity or individual.
- The counterparty has an apparent connection to a sanctioned entity, including but not limited to being part of the same corporate family.
- The counterparty or an agent is reluctant to provide routine information about (i) the counterparty's identity; (ii) the end use of the product; (iii) whether the product will be exported or used domestically.
- Payment terms or method that are not through normal banking channels, such as cash for items not normally sold for cash, or are otherwise, to the Company's reasonable understanding, abnormal.
- Transport or delivery terms are non-INCOTERM or are vague as to origin of the product, load location, manner of transport, place of delivery, or end-use of product.
- The counterparty is not, or claims it is not, familiar with the product and/or its uses.
- The product does not fit with the counterparty's usual activities or location.
- The consignee has a different name or location than the business partner or ultimate end user.
- Volumes wholly inconsistent with the Company's reasonable understanding of the market size.
- Invoicing, shipping, or packaging requests that are, to the Company's reasonable understanding, abnormal.
- Transportation routes that are, to the Company's reasonable understanding, abnormal.
- Any suspicion of or evidence to suggest a military related end-use for the benefit of a sanctioned party.

Shipping Red Flags

- Indications of falsified or inconsistent cargo or vessel documents.
- Reluctance by the counterparty or agent to provide additional information or documentation upon request, such as available ship-to-ship (STS) history, ownership history, flag registration history, or insurance-related records.
- Flagging in a high-risk jurisdiction.[10]

[10] This includes, but is not limited to, Cambodia, Eswatini, Gabon, Guinea-Bissau, St Kitts and Nevis, Comoros, Palau, Tuvalu, Liberia, Marshall Islands, Panama, Russia, and the United Arab Emirates.

- Vessel location and identification data that is, to the Company's reasonable understanding, abnormal, particularly if the vessel appears close to a high-risk jurisdiction.
- Frequent renaming of vessel.
- Vessel is owned or controlled by owners known to own other sanctioned vessels.
- Vessel was last loaded via STS transfer, with no information about source of product loaded at STS location.
- Complex and abnormal vessel ownership and management structures.

APPENDIX B: Transaction Due Diligence Checklist

Counterparty:
Vessel:
Subject Matter:
Transaction Date:

Counterparty Due Diligence

The Counterparty has completed the KYC Questionnaire, including providing relevant documents, which are saved in the Transaction File.

The Sanctions Screen of the Counterparty and any individual or entity having 20% or more direct or indirect ownership in the Counterparty is complete and returned negative. Results are saved in the Transaction File.

In addition to the Counterparty, Sanctions Screens were performed on the following individual(s)/entity(ies) and returned negative:

Open-source research conducted on the Counterparty.
No red flags were observed.
Red flags were observed, escalated, and resolved, as documented in the Transaction File.

Vessel Due Diligence
Sanctions Screen on the vessel name returned negative. Results are saved in the Transaction File.

The Vessel is not flagged in a sanctioned country.

Sanctions Screen of the vessel's operator/manager returned negative. Results are saved in the Transaction File.

Sanctions Screen of each vessel owner (up to the ultimate beneficial owner) returned negative. Results are saved in the Transaction File.

Last ten ports of call verified through a reliable third-party intelligence system returned negative for sanctioned ports. Results are saved in the Transaction File.

Open-source research conducted on the Vessel.

No red flags were observed.

Red flags were observed, escalated, and resolved, as documented in the Transaction File.