Anti-Money Laundering and Sanctions Policy

Document Version No.: 1.4

Release Date: 5th June 2026

Date	Version No.	Prepared By	Reviewed By	Approved By	Summary of Changes
5-June-26	1.4	Vaishali Gore	Rajashree Laad	Uma Thomas	Updated compliance_reporting@hexaware.com in stead of complianceofficer@hexaware.com
3rd Nov 25	1.3	Vaishali Gore	Rajashree Laad	Uma Thomas	Updated Section 1- Policy Statement - LODR regulations Updated Section 3 Definition on- FATF Updated Section 6.2 "Monitoring of transaction" to include Financial & Non-Financial controls

Table of Contents

1. Policy Statement 3
2. Purpose 3
3. Definitions 3
4. Applicability of the policy 7
5. Roles and Responsibilities 8
6. Due Diligence of third parties or customers: 9
6.1. New Customer or third-party acceptance: 9
6.2. Monitoring of transactions: 11
6.3. Periodic review: 12
7. Reporting requirements 13
8. Employee training and awareness 13
9. Maintenance of records 13
10. Independent Auditing / Testing 14
11. Disciplinary Measures 14
12. Exceptions and Exemptions 15
14. Annexure 16

1. Policy Statement

Hexaware Technologies Limited (the use of "Hexaware" or "company" hereinafter, implies Hexaware Technologies Limited and all companies wholly or partially owned by Hexaware), aims to adhere to the highest standards of professional and ethical standards. The Company endeavors to conduct its business dealings and affairs in a fair and transparent manner, adopting the highest standards of professionalism in compliance with applicable Anti Money Laundering (AML) / Counter Terrorist Financing (CFT) Laws, the global Sanctions laws and regulations of the United Nations (UN), the European Union (EU), Financial Action Task Force (FATF), The Office of Foreign Assets Control (OFAC), the United States (US) and in other countries in which Hexaware operates in.

The fight against money laundering and terrorist financing is a priority for the Company. While the Company does not have reporting obligations under the Prevention of Money Laundering Act, 2002 (PMLA), the Company shall comply with certain requirements as discussed in this Anti-Money Laundering (AML) & Sanctions Policy (the "Policy") which provides guidelines to its Employees, customers, and third parties through various guiding resources which prevent them from dealing in money laundering or terrorist financing activities and complying with the applicable global Sanctions laws and regulations.

This policy forms an integral part of the Code of Conduct and should be read in conjunction with The Whistle blower policy, The Anti- Bribery and Anti- Corruption Policy, The Third-party policy document along with SEBI Listing Obligations and Disclosure Requirements (LODR) Regulations, 2015; and any guidance published pursuant to this policy and other relevant policies as may be implemented in future.

2. Purpose

The purpose of this policy is:

- To create awareness among employees about AML/ CFT laws & global sanctions Laws, Rules and Regulations .
- To provide guidance for the customers, and third party's acceptance (due diligence) process with regards to AML and Economic Sanctions.
- To establish provisions that will mitigate the Company's involvement in any money laundering or terrorist financing activity or in any restricted trade activity or with a restricted entity/ country, directly or indirectly.
- To protect and enhance the reputation of the Company.

3. Definitions

a) For the purpose of this Policy, Company Management includes the CEO and Executive Committee of the Company. "**Director**" means every Director of Hexaware, past or present.

b) "**Employee**" means any person hired to perform a job or service for Hexaware, and one who is directly employed or hired on a contractual basis. This includes all individuals working for Hexaware, whether in India or abroad, at all levels and grades, including the Leadership Team, Directors, senior executives, officers, employees (whether permanent, fixed-term or temporary), trainees, seconded staff, or any other person associated with the Company and their relatives.

a) **"Third parties"** - Includes entities and individuals, other than the Employees, with whom the Company has business relationships including but not limited to consultants, intermediaries, representatives, suppliers, contractors, subcontractors, agents, distributors, third party influencers/ rainmakers, business partners and advisors which enable them to operate by providing services, supplies materials and/or interacts with the Government or with others on behalf of the Company to achieve the contracted business.

c) **"Money Laundering"** - Money laundering is the process by which individuals or entities attempt to conceal the true origin and ownership of the proceeds of criminally derived funds or assets. Money Laundering involves three steps:

- "Placement" - Placing the "dirty money" into the legitimate financial system. For example: the commingling of illegitimate funds with legitimate funds such as placing the cash from illegal sales into the cash-intensive locally owned restaurant.

- "Layering" - Concealing the source of the money through a series of transactions and bookkeeping tricks. For example, converting the cash placed into monetary instruments.

- "Integration" – This is the movement of previously laundered money into the economy mainly through the banking system and thus such money appears to be normal business earnings. For example, purchasing luxury assets like property, artwork, jewellery, or high-end automobiles.

d) **"Terrorist Financing"** - Terrorist financing is the financing of terrorist acts, or terrorists and terrorist organizations. Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities include (but are not limited to) extortion, kidnapping, narcotics trafficking, smuggling, fraud, theft, robbery, identity theft, improper use of charitable or relief funds, etc.

e) **"Beneficial Owner (BO)"** - Beneficial owner refers to the natural person(s) who ultimately owns or controls the third party/customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over the third party/customer.

f) **"Blocked Assets"** - Blocked Assets restrict asset owners from unlimited and unrestricted use of their assets. Assets may be blocked or limited for a variety of reasons, including internal firm policy, external regulations, or via a court order or legal decision. An Asset that has become completely blocked is referred to as a frozen asset.

g) **"Comprehensive Sanction"** - Comprehensive sanctions include broad-based trade restrictions and prohibit commercial activity with an entire country.

h) **"Customers"** - Includes all clients, individuals/legal entities, and others directly engaged by Hexaware and to whom they provide its solutions and services,

i) **"Related Parties"** - Related parties are those individuals or entities who have relationships with the third parties/customers such as the power of attorney holders, executive management (e.g. Chief Executive Officer (CEO), Chief Financial Officer (CFO), Directors), Board of Directors, shareholders, etc.

b) **"Politically Exposed Person (PEP)"** - "PEP" means an individual who are or have been entrusted with prominent public functions and includes governors of state, members of parliament, military officers, senior government and judicial executives and heads of local bodies including municipal corporations among others. PEP generally represents a higher risk for potential involvement in bribery and corruption by virtue of their positions and the influence that they may hold. Examples include:

- Members of Legislative Bodies: Member of Parliament, Legislative Assembly, Legislative Council
- Security Forces: High ranking officials of Military, Navy, Airforce, Law Enforcement (Police), Investigation Agencies (CBI)
- Executive Bodies: President, Governors, Prime Minister, Chief Ministers, Union Ministers, Council of Ministers, Minister of State and Deputy Ministers, Minister of State/Department (including secretary to ministers)
- Judicial Bodies: Attorney general, Solicitor General, Election Commissioner, Central Vigilance Commissioner, Judges of Supreme Court and High Courts etc.
- Bureaucrats: Members of the Administrative, Management or Supervisory Bodies (IAS, IPS, IRS and Officers employed through Public Service Commission).
- Affiliation with a political party, as identified through keywords-based searches and reported in the media. Close Associate/ Collaborators- A person who is widely and publicly known to maintain an unusually close relationship with the political figure and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the political figure.
- Specifically, the following are considered close collaborators:
- Natural persons who are known to have a partnership or joint ownership in legal entities governed by private law or in arrangements without legal personality, who are authorized representatives, or have any other close relationship of public knowledge with an exposed person politically; and
- Natural persons who have control of legal entities governed by private law or in arrangements without legal personality known to have been created for the benefit of a politically exposed person.

- Director with a state-owned entity or entity indirectly owned by a government body/ministry
- Immediate family member (parents, spouse, and children) of a known PEP, as reported in databases and/or media sources
- Any close Business associate of a PEP, as reported in databases and/or media sources (as identified through keywords-based searches)

j) **"Source of Funds**" - Source of funds refers to the origin of the funds which are used in a particular business transaction between a customer/third party and the Company. For e.g. Third party receiving funds from an entity located in the Cayman Islands.

k) **"Source of Wealth" -** Source of wealth describes how a third party or beneficial owner acquired their total wealth. For e.g., Third party's source of wealth is from family inheritance or house sale.

l) **"Trade Based Money Laundering (TBML)**" - As per FATF, Trade Based Money Laundering (TBML) refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origin or finance their activities.

m) **"FIU**" - Financial Intelligence Unit - India (FIU-IND) is the central, national agency responsible for receiving, processing, analyzing, and disseminating information relating to suspect financial transactions to enforcement agencies and foreign FIUs.

https://dor.gov.in/preventionofmoneylaundering/financial-intelligence-unit-india-fiu-ind

n) **"OFAC"** - The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information

o) **"Restricted entity/country**" - A restricted entity or a country means any entity/ country which is subject to integrated and country-wide restrictions under global Sanctions laws and regulations of the United Nations (UN), the European Union (EU), the United States (US), and other countries in which Hexaware operates in.

p) **"Sanctions" -** Sanctions refer to laws and regulations relating to economic and financial sanctions and trade embargoes which consist of restrictions and prohibitions on transactions with certain countries, entities, individuals, vessels, and aircraft.

q) **"Sanctions Screening**" - The review process is completed prior to or during a transaction in which individuals, businesses and/or entities that have any interest in the transaction are reviewed, contributing to the mitigation of reputational risks and of the risk of Sanctions violations.

r) **"Target Sanction"** - Target-based or Sectorial Sanction targets specific sectors of the sanctioned country or regime's economy and targets entities/individuals that evade or circumvent the sanction programs.

s) **"UNSC"** - The United Nations Security Council is the premier global body for maintaining international peace and security; UN sanctions are diplomatic decisions enforced by the United Nations organizations and states against other states, entities, or individuals.

https://www.un.org/securitycouncil/sanctions/information.

t) **FATF – Financial Action Task Force an inter-governmental body that sets global standards to combat money laundering, terrorist financing, and the financing of weapons of mass destruction. It has a mandate to protect the global financial system.**

https://www.fatf-gafi.org/

4. Applicability of the policy

This policy is applicable globally to Hexaware Technologies Limited, its subsidiaries and affiliates.

This policy applies to all Company directors, officers, employees, contractors, consultants, vendors, and other persons working under the Company's managerial supervision, including all individuals employed by any entity owned and/or controlled by the Company (the "Hexaware team").

In addition, this policy also applies to customers, third parties, or any natural or legal persons who have agreed to become a buyer/supplier of the Company's products or services or would agree to become a buyer/supplier of the Company's products or services in future. All such persons have an important role to play in safeguarding Hexaware's reputation, legal and financial interests, and upholding its policies. All employees play a key role in helping the Company comply with the applicable regulations.

The management will not criticize any loss of business resulting from adherence to this Policy. No employee or contractor will suffer as a consequence of bringing to the attention of the Board or senior management, in good faith, a known or suspected breach of this Policy. Also, employees and contractors will not suffer any adverse employment decisions for abiding by this Policy. Refer to Hexaware's Whistle Blower Policy on raising suspicion to the company.

Employees' Obligations: It is the responsibility of all employees and executives of Hexaware and its controlled entities to be committed to the rules established in this Policy and are responsible for disseminating following the guidelines contained herein. Any questions or additional guidance regarding this policy or application procedures should be directed to the Compliance Department (complian_reporting@hexaware.com)

5. Roles and Responsibilities

In order to ensure effective implementation of the provisions of this policy, the Company shall assign roles and responsibilities as mentioned below:

a) **Board of Directors:** The Board of Directors shall create a culture of compliance to ensure adherence to the Company's AML & Sanctions Policy by providing an oversight of AML and Sanctions compliance framework.

b) **Head of Compliance, Procurement & Finance Department:** The Head of the Compliance, Procurement & Finance Department shall be responsible to ensure performance of the key responsibilities of the Compliance, Procurement & Finance Department defined under this policy, while also ensuring appropriate segregation of duties between the Compliance, Procurement & Finance Department related to their key responsibilities defined under this policy.

c) **Compliance Department:** The compliance department will perform the following activities:

- Promote compliance with the AML & Sanctions policy and supervise all AML and sanctions-related matters within the Company.
- Act as the point of contact for all communication with the Board of Directors of the Company in relation to AML & sanctions-related matters.
- Review escalations from Finance and Procurement that entail suspicious activity/transactions and provide appropriate resolution for the same and proactively identify, monitor investigate, and report suspected violations.
- Report suspicious customers, or third party's activity/transactions to the Board of Directors.
- Supervise the maintenance of the records as required in this policy.
- Ensuring that training and awareness materials are developed and delivered in relation to this Policy and that management and employees are provided with the training.
- Take necessary remedial actions, arising from internal audit inspection, and Compliance reviews with matters relating to AML & Sanctions compliance.
- Updating policies and procedures for economic Sanctions compliance reflecting current regulatory requirements as applicable.
- Setting the appropriate tone at the top and ensuring that all management and employees do the same;
- Fostering an open environment for employees to discuss potential violations of this Policy.
- Regularly review the policies and procedures to ensure their effectiveness.

d) **Procurement & Finance Department:** The Procurement & Finance Department of the Company shall perform the following key responsibilities:

- The Procurement & Finance Department shall be autonomous in their decisions while assessing a potentially suspicious customer's or third party's activity/transaction.
- Oversee the customers, and third party's due diligence process and ongoing monitoring of the business relationship.

e) **Employees of the Company:** In relation to the AML Policy, all Employees of the Company shall comply with the following responsibilities-

- Understand this policy and in case of any doubt, approach the Compliance department for clarification.
- Any red flag or suspicious transaction or suspicious activity identified shall be reported to the Compliance department using the Template for Internal Suspicious Transaction Reporting or any other appropriate channels as advised by the Code of Conduct Policy.
- Employees shall not disclose any money laundering or terrorist financing-related suspicion (escalated to the Compliance Department) to the customers, or the third party.

6. Due Diligence of third parties or customers:

6.1. New Customer or third-party acceptance:

The company shall perform due diligence with regards to AML and Sanctions compliance on all the customers and third parties before starting a business relationship with them or conducting any transactions with them.

KYC due diligence- As part of initial KYC information gathering, the Company shall seek complete visibility on the customers, and third parties; their business operations (major source of generating business/funds), jurisdictions in which they operate, and related parties with whom they deal with, for services provided by Hexaware. Therefore, the onboarding process shall include the gathering of the following information:

- Details of the customer/third parties and its beneficial owners and key personnel including related parties;
- Identity information of any related party or person that is authorized to act on behalf of the customer/ third party.
- Identity (names and verification information) of all parties involved in the entire lifecycle of the business relationship and other parties mentioned in the contracts. In case, the parties involved are body corporates, the details of the Group company should be gathered
- Customer's/ third party's locations of operations.

The due diligence process enables the company to analyze and understand the business background of its customers and third parties; negative news/adverse media positive screening hits if any and also wade away any vulnerabilities of money laundering. In addition, the due diligence process should include the gathering of information about the association of the customers or third parties with politically exposed persons (PEP) to uncover increased risks such as holding a position that can be abused for the purpose of laundering funds.

Sanction screening of new customer or third party- Based on the information gathered during KYC due diligence process prior to commencing any business relationship, Finance and Procurement teams will be responsible for screening new customers, third parties, and associated entities, including any authorized signatories or other related parties, against applicable jurisdiction sanctions lists. (Please refer to the AML and Sanctions Compliance Procedures document for a detailed process on acceptance of a new customer, or a third party and refer to Annexure B for country-wise sanction lists)

If the customer or third party is a natural person: full name, date of birth, nationality, and address should be captured to perform screening, and the name of the entity with which it is associated to (if any);

While establishing customers, and third parties' relationships, Finance and Procurement teams shall observe the following provisions-

- Restrict any relationships in jurisdictions where comprehensive Sanctions are applicable or if the customer or third party is a sanctioned entity or an individual,
- Restrict the customer or the third party with an anonymous or fictitious name
- Enhanced Due diligence for the customer or the third party based in jurisdictions that have target-based or comprehensive Sanctions. Onboarding or execution of transactions with such parties shall be subject to the Compliance department's approval.
- Customer or third party for whom appropriate due diligence measures could not be applied due to lack of verifiable documents or on account of non-cooperation of the party or non-reliability of the documents/information furnished by the party such cases shall be subject to the Compliance department's approval
- Conduct Negative News/Adverse Media screening on the customer and evaluate any positive hits

Refer to Annexure B for the list of references and links on comprehensive and target-based sanctions, and guidelines shared by the Sanction Regulatory Authorities. Any potential AML or Sanctions finding/incident shall immediately be escalated to the Compliance Department. The Compliance Department shall conduct a review and investigate the escalated incident to determine appropriate next steps. In case the compliance department opines to exit the relationship with the customer or the third party, they may refer to the exit guidance in "Third Party Management Policy".

Note: The guidelines on comprehensive and target-based sanctions are updated from time to time, therefore the Compliance department will ensure the latest guidelines are followed.

6.2. Monitoring of transactions:

AML and Sanctions laws impose certain prohibitions and restrictions that should be considered before initiating any transaction. These include -

- Prohibiting customer relationships or engaging in transactions or business activity (including certain countries, territories, or governments).
- Restricting certain transactions and business activity which involve, directly or indirectly, certain countries, governments individuals, entities, or industry sectors.

The Hexaware Finance and Compliance team shall monitor the business transactions to ensure compliance with applicable prohibitions and restrictions.

Each transaction shall be reviewed to ensure the following-

- Sanctions screening for parties involved, with whom the transaction is agreed upon and the nature of transaction to be entered into. If there are related parties involved, such parties should be screened as well against the Sanctions lists as mentioned in Annexure B
- Ensure that financial transactions/operations (including contact with financial institutions, usage of a certain currency, segregation of funds) are in line with economic trade sanctions regulations and guidance issued by OFAC, UN, EU, and any applicable local jurisdictions. This will require screening of product/s as per the sanction's regulation of the local jurisdiction.
- Ensure that all legal licenses are obtained when required.

This section should be read and understood in conjunction with the AML and Sanctions compliance procedures document, which encompasses details of AML and Sanction laws and regulations applicable to Hexaware. The document explicitly covers sanctioned countries and refers to the search list provided by each Sanctions regulatory body

Any potential AML or Sanctions finding/incident shall immediately be escalated to the Compliance Department during the monitoring of transactions. The Compliance Department shall conduct a review and investigate the escalated incident to determine appropriate next steps. In case the compliance department opines to exit the relationship with the customer or the third party, they may refer to the exit guidance in "Third Party Management Policy".

In addition to this, the organization shall implement financial & non financial controls to ensure effectiveness of Anti-Bribery & Anti-Corruption & Anti-Money Laundering framework which is aligned to ISO 37001 Anti- Bribery Management Systems

Some of the Financial controls are listed below*-

- Segregation of duties
- Delegation of authorities
- Revalidating the transaction for details
- Requiring the appropriate supporting documentation to be annexed to payment approvals

- Periodic and independent financial audits and changing, on a regular basis, the person or the organization that carries out the audit.

*The list is not exhaustive

Some of the non-financial controls are listed below*-

- Working with suppliers/third parties from approved supplier list only
- Conducting Due diligence of the third party before on-boarding
- Assessing whether the services were properly carried out by the third partyAwarding contracts, where possible and reasonable, only after a fair and, where appropriate, transparent competitive tender process between at least three competitors has taken place.

6.3. Periodic review:

Periodic screening is the process of screening the information which the Company collects and maintains on the parties it does business with. This includes identifying and verifying customer/third parties information including its associated parties and beneficial owners, that may present a relevant AML and Sanctions risk.

Periodic screening shall be performed by the Finance & Procurement team and should include the screening of the customer, authorized signatories, and all key personnel as described in the section above based on below conditions-

- Whenever the Hexaware team becomes aware that there is a change in the sanctions list e.g., a target has been added or removed from the list.

- At the time of contract renewal from the customer or the third party

- Whenever the Hexaware team becomes aware of the change in the directorship, change in the location/address of the company, change in the entity name, or any changes in the shareholding pattern etc.

Timelines for carrying out the verification - Applies to new party acceptance, transaction monitoring, and periodic review and screening -

- New details must be verified within two business days through manual verification.

- For details, already present in Hexaware internal systems, preliminary (annual) checks must be performed prior to entering into a contract.
- Payment transactions – For one-time partners (where applicable), data verification must be performed prior to making the payments

Any potential AML or Sanctions finding/incident shall immediately be escalated to the Compliance Department during the periodic review. The Compliance Department shall conduct a review and investigate the escalated incident to determine appropriate next steps. In case the compliance department opines to exit the relationship with the customer or the third party, they may refer to the exit guidance in “Third Party Management Policy”.

Aggravated cases of breach of this AML Policy shall be escalated to the Board of Directors through the (Chief Risk Officer).

7. Reporting requirements

All Hexaware employees are responsible for preventing, detecting, and reporting instances of the suspected activity or business transaction linked to sanctioned parties, AML activities, or any other suspicious activity.

If any Company personnel or third party becomes aware of any actual or suspected violation of this Policy or receives any complaint, they shall report using the reporting mechanisms as detailed in the Whistle-Blower Policy or in any other manner.

Upon detection of red flags or suspicious customers, or third-party activity/transactions, Employees shall disclose the matter to the Compliance Department at complian_reporting@hexaware.com without any undue delay using the Template for Internal Suspicious Transaction Reporting. If it is established that the customer, third party or the transaction is suspicious, the Compliance department will report the incident to senior management for the next steps, and internally the firm will decide on the reporting on a case-to-case basis. For more details on the escalation and investigation procedures, refer to the AML and Sanctions compliance procedures.

Complaints received through different channels shall be investigated in alignment with the Company's Whistle-Blower Policy. Any investigation required shall be conducted without regard to the length of service, position/title, or relationship with the Company of any party, including any persons suspected of breaches of this Policy.

In addition, an employee can also report such matters using other appropriate channels as mentioned in Hexaware's Code of Conduct.

8. Employee training and awareness

The Company shall ensure an appropriate culture by providing regular training to Employees on the policies and procedures as well as the rules and requirements of applicable laws. Such training is to be provided at the time of joining and annually thereafter.

This Policy shall be accessible to all the Employees on the Company's intranet.

The Company shall ensure that all contracts with customers, and third parties include Anti-Money Laundering and Sanctions compliance clauses and obtain an Anti-Money Laundering and Sanctions compliance undertaking or declaration from the customers, and third parties asking for disclosure of any past or current matter in relation to incidence of money laundering or sanctions escalation in the respective company. The contract should also include the requirement for disclosure of any incident of money laundering or sanctions, while the contract is in effect, to the Company.

9. Maintenance of records

The Company shall collect certain information as part of the relationship from the customer/third parties including but not limited to:

- Business agreements between customers, third parties and other parties,
- Due Diligence information obtained at the onset and during the course of a business relationship for customers, and third parties,
- Certain transaction activities, including domestic and international fund transfers with Hexaware
- Transaction details such as Proforma Invoice, contracts, transaction details with customers and third parties etc.

All such records including customers' AML and Sanction's screening and transactions monitoring shall be maintained for at least five years after the date of the transaction. In the case of blocked assets/funds, records must be maintained for the period the assets/funds are blocked and for five years after the date the assets are unblocked.

Records must be maintained in a manner such that they are readily retrievable and accessible in a reasonable period for internal reviews, or in response to law enforcement or regulatory requirements.

Specifically, the following records should be maintained -

- records related to AML and Sanction screenings performed on customers, third parties and their associated parties including beneficial owners and related parties.
- the nature of the transaction.
- the amount of the transaction and the currency in which it was denominated.
- the date on which the transaction was conducted.
- the parties to the transaction, and countries involved.
- Any approval documents received from any government or jurisdictional authorities, etc., if applicable for the aforesaid business transactions

10. Independent Auditing / Testing

The company shall include the Anti-Money Laundering & Sanctions Policy and Procedures as part of its Internal Audit plan.

11. Disciplinary Measures

The Company shall have an irreconcilable attitude to any forms and manifestations of misconduct at all levels of the Corporate Governance. As, violating AML and Sanctions could expose the Company to civil and criminal fines and a loss of certain privileges, in addition to potentially exposing individual Hexaware Team members to monetary penalties and even imprisonment. In addition, violating AML and Sanctions laws could impact Hexaware's relationships with counterparties, harming its reputation and ability to conduct business.

The Company shall investigate all reasonably substantiated reports of violations of this Policy to prevent and combat money laundering and to ensure Sanction compliance.

Employees must cooperate fully and openly with any internal investigation into alleged or suspected money laundering activity, sanction's non-compliance, or breach of this Policy of any kind.

Any breach of this Policy or failure to cooperate or to provide truthful information shall be treated as misconduct under the Disciplinary Policy and/or other applicable laws. In case of default by the customer, or a third party the action shall be taken considering the legal recourse available.

12. Exceptions and Exemptions

Exemptions or exceptions to this Policy shall be granted rarely and would be supported by documentation detailing the evidence and rationale behind the exemption or exception. Any exemption or exception to this Policy must be approved by the Compliance Department.

Associated Documents

Hex 5909 Template for Internal Suspicious Transaction Reporting

13. Adaptation and local laws

The principles for bribery and corruption laws may need some adaptation to comply with all applicable local laws, rules and regulations. In the event of any conflict between the provisions of this policy and any applicable local laws or regulation, the more stringent requirement shall prevail. In case of any doubt, please reach out to compliance_reporting@hexaware.com. It will be reviewed y Legal and Compliance and the final adaptation will be approved by the Chief Risk Officer.

14. Annexure

Reference to country wise sanction lists -

S.N.	Country Names	Applicable Sanction lists
1	North America - Mexico, USA, Canada	**OFAC-** Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC): Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions OFAC Sanction Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **UN Sanctions List-** UN sanction lists are available on https://scsanctions.un.org/search/ Information on UN Security Council Sanctions : https://www.un.org/securitycouncil/sanctions/information **Consolidated Canadian autonomous Sanction List:** Consolidated Canadian Autonomous Sanctions List includes individuals and entities subject to specific sanctions regulations made under the Special Economic Measures Act (SEMA) and the Justice for Victims of Corrupt Foreign Officials Act (JVCFOA). https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng **Consolidated Search List** (This search covers OFAC and other US sanctions)**:** https://www.trade.gov/data-visualization/csl-search

S.N.	Country Names	Applicable Sanction lists
2	South America- Brazil, Argentina	**OFAC-** 3. Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC): Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions OFAC Sanction Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **UN Sanctions List-** UN sanction lists are available on https://scsanctions.un.org/search/ Information on UN Security Council Sanctions: https://www.un.org/securitycouncil/sanctions/information **Consolidated Search List (This search covers OFAC and other US sanctions) :** https://www.trade.gov/data-visualization/csl-search
3	Europe - UK, Belgium, Netherlands, Germany, Poland Latvia, France, Spain, Switzerland , Denmark,	**UN sanction** lists are available on https://scsanctions.un.org/search/ Information on UN Security Council Sanctions : https://www.un.org/securitycouncil/sanctions/information **European Union sanction lists** and measures are available on http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf Map of sanctions currently applied in the EU: www.sanctionsmap.eu **Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC)**: Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions.

S.N.	Country Names	Applicable Sanction lists
	Austria, Estonia, Sweden	https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions **OFAC Sanction:** Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **Consolidated Search List (This search covers OFAC and other US sanctions)** https://www.trade.gov/data-visualization/csl-search **UK Sanctions list:** https://www.gov.uk/government/publications/the-uk-sanctions-list
4	A/sia - China, Philippines, UAE, India, Japan, Hong Kong, Singapore	**OFAC-** Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC): Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions OFAC Sanction Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **UN Sanctions List-** UN sanction lists are available on https://scsanctions.un.org/search/

S.N.	Country Names	Applicable Sanction lists
		Information on UN Security Council Sanctions : https://www.un.org/securitycouncil/sanctions/information **Consolidated Search List (This search covers OFAC and other US sanctions)**: https://www.trade.gov/data-visualization/csl-search
i	UAE	**Additional checks for UAE in addition to sanction links that are applicable for Asia –** **UAE- Control lists on goods:** https://www.uaeiec.gov.ae/en-us/control-list-good Local Terrorist and UN Consolidated list for UAE: https://www.uaeiec.gov.ae/en-us/un-page?p=1
ii	India	**Additional checks for India in addition to sanction links that are applicable for Asia –** Indian regulatory requirement abides to **Unlawful Activities (Prevention) Act (UAPA)**, 1967, approved by the United Nations Security Council Unlawful Activities (Prevention) Act is an Indian law to provide for the more effective prevention of certain unlawful activities of individuals and associations, and for dealing with terrorist activities, and for matters connected therewith. The below Indian lists are also a part of UN sanctions list which will be checked for sanctions (**"ISIL (Da'esh) & Al-Qaida Sanctions List**", and "**1988 Sanctions List associated with the Taliban**") https://scsanctions.un.org/3ppp1en-taliban.html https://scsanctions.un.org/ohz5jen-al-qaida.html https://rbidocs.rbi.org.in/rdocs/content/pdfs/UNSCR29072022.pdf

S.N.	Country Names	Applicable Sanction lists
iii	Singapore	**Additional checks for Singapore in addition to sanction links that are applicable for Asia –** **MAS** - As a member state of the UN, Singapore implements UN sanctions through the United Nations Act (Cap. 339) (UNA), UNA which applies to non-financial institutions and individuals, and, through regulations issued by the Monetary Authority of Singapore (MAS) under the MAS Act, which apply to financial institutions https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities
iv	Hong Kong	**Additional checks for Hong Kong in addition to sanction links that are applicable for Asia –** **Hongkong:** https://www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html
5	Australia	**OFAC-** Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC): Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions OFAC Sanction Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **UN Sanctions List-** UN sanction lists are available on https://scsanctions.un.org/search/ Information on UN Security Council Sanctions: https://www.un.org/securitycouncil/sanctions/information **Consolidated Search List (This search covers OFAC and other US sanctions):** https://www.trade.gov/data-visualization/csl-search

S.N.	Country Names	Applicable Sanction lists
		Consolidated list from DFAT: The Consolidated List is a list of all persons and entities listed under Australian sanctions laws. Listed persons and entities are subject to targeted financial sanctions. Listed persons may also be subject to travel bans. https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list
6	Africa	**OFAC-** Sanction lists and measures imposed by the Office of Foreign Assets Control (OFAC): Basic Information on OFAC and Sanctions, refer to the below link for the comprehensive and selective sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions OFAC Sanction Search list including Consolidated Non-SDN List and SDN and Blocked person list: https://sanctionssearch.ofac.treas.gov/ https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists **UN Sanctions List-**

S.N.	Country Names	Applicable Sanction lists
		UN sanction lists are available on https://scsanctions.un.org/search/ Information on UN Security Council Sanctions : https://www.un.org/securitycouncil/sanctions/information **Consolidated Search List** (This search covers OFAC and other US sanctions): https://www.trade.gov/data-visualization/csl-search