Anti-Money Laundering Policy-Global

Revision History:

Version	From	To	Description	Author	Approved By
1	12 Feb 2013	09 Dec 2017	First Copy	Global Compliance Team	Global Compliance Head
2	10 Dec 2017	28 Feb 2019	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
3	01 Mar 2019	28 May 2020	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
4	29 May 2020	03 Sep 2020	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
5	04 Sep 2020	14 Mar 2022	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
6	15 Mar 2022	31 Jul 2022	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
7	01 Aug 2022	04 Oct 2022	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
8	05 Oct 2022	14 Jun 2023	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
9	15 Jun 2023	25 Aug 2024	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head
10	26 Aug 2024	-	Revision	HR Policy &Compliance CoE	HR Policy &Compliance CoE Head

Objective:

The purpose of this Anti-Money Laundering Policy (this "**Policy**") is to state HCLTech's zero-tolerance approach to money laundering and provide guidance/framework to HCL Technologies Limited and/ or its affiliated entities and subsidiaries (hereinafter collectively "**HCLTech**") to understand HCLTech's obligations under anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") laws, to ensure transparency in all HCLTech financial transactions, to help HCLTech manage associated risks, and to put in place effective AML and CTF controls in order to ensure that HCLTech:

o Avoids being used as a vehicle for money laundering

o Conducts adequate due diligence on new and existing counterparty and establishes sound Know-Your-Customer ("**KYC"**) norms; and

o Imparts continuous training to all employees in relevant functions on this Policy and establishes good reporting procedures.

HCLTech is committed to conduct business in an ethical and lawful manner, and AML/CTF laws are critical to preventing criminals from utilising funds generated by criminal activity and preventing the financing of terrorism.

There are severe civil and criminal penalties for violations of AML/CTF laws. These can involve significant fines for HCLTech and its personnel. In the worst case, it could also involve prison sentences and extradition risks for individuals involved in a breach. **A breach may also have a significant reputational impact and can lead to a loss of business and the withdrawal of the HCLTech's banking facilities.**

Scope:

This Policy applies to all HCLTech employees, including employees, officers, directors, temporary staff and third-party contractors (such as distributors and representatives) ("**HCLTech Personnel and Associates**"). To the extent any of the HCLTech regulated entities, which have additional legal and regulatory obligations or have more stringent policies and procedures specific to such organization, the same must be consulted to ascertain obligations and requirements for such regulated entities. These entities include, but are not limited to:

- HCL Insurance BPO Services Limited
- HCL Great Britain Limited
- HCL New Zealand (NZ) Limited
- HCL Lending Solutions LLC

PolicyDetails:

3. Definitions

"**Money Laundering**" is any transaction or series of transactions undertaken to conceal or disguise the nature and source of funds that have been obtained from illegal activity to make the funds appear legitimate. "**Terrorist Financing**" is the financing of terrorist acts, terrorists, or terrorist organizations.

4. Ownership and Responsibilities of Employees

All HCLTech Personnel and Associates must:

- Read, comply with, and understand how this Policy applies to their job functions;
- Ask their supervisor or HCLTech's Compliance Department for guidance when they are uncertain about how to comply with this Policy;
- Complete all required training and certifications related to this Policy, if any; and
- Report violations or potential violations in accordance with Section 6 of this Policy.

Compliance with this Policy is mandatory. If local law imposes stricter requirements than those described in

this Policy, HCLTech Personnel and Associates must comply with those requirements under law and/or any additional HCLTech policies enforcing the same (see Section 2. Scope above).
The respective department heads are also responsible for ensuring adherence to this Policy. They are to make their subordinates aware of the Policy and suggest any additional training programs needed for their department

5. Policy Statement

HCLTech complies with all AML and CTF laws applicable to our business wherever we do business and takes steps to ensure that we do not engage with counterparties – including customers or suppliers – who may seek to use legitimate business activities with HCLTech as a means to facilitate laundering activities, terrorist financing, or otherwise engage in transactions with HCLTech involving criminal proceeds.

5.1 What is Money Laundering

Money laundering occurs when a party engages in acts designed to conceal or disguise the true origins of criminally derived proceeds so unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. The main objective of the money launderer is to transform dirty money into seemingly clean money or other assets. Generally, money laundering occurs in three stages:

1. **Placement:** Cash generated from criminal and/or illegal activities is converted into monetary instruments, such as money orders, traveler's checks or deposited into accounts at financial institutions.
2. **Layering**: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its origin.
3. **Integration**: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal and/or illegal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used to finance terrorist purposes. Money laundering is often an element of terrorist financing.

5.2 Potential Criminal Exposure

Money laundering and terrorist financing are illegal. Involvement at the "integration" stage as a recipient of criminal proceeds exposes HCLTech and HCLTech Personnel and Associates to possible liability under the law. HCLTech could be liable if it engages in a monetary transaction in criminally derived property with the knowledge that such property came from unlawful activity. HCLTech or HCLTech Personnel and Associates could also violate various criminal laws where we know, or should have known, that a party with whom we are doing business has engaged in unlawful activity and tries to utilize transactions with HCLTech to conceal that activity. **In the worst case, it could also involve prison sentences and extradition risks for individuals involved in a breach**. AML/CTF violations may also have a significant reputational impact and can lead to a loss of business and the withdrawal of the HCLTech's banking facilities.
As such, it is critical that HCLTech does not engage in transactions with third parties who could cause financial institutions with whom we do business to question the integrity of the activity in our accounts, jeopardizing our critical relationships with those financial institutions. In order to mitigate these risks, it is imperative that HCLTech.

- Conducts risk-based due diligence on certain counterparties with whom we transact to identify those who may engage in illegal activity or who otherwise may expose HCLTech to increased money-laundering risk; and
- Monitors monetary transactions between HCLTech and its counterparties and account activity to identify transactions that could pose heightened money laundering risk.

5.3 Risk Assessment & Register

HCLTech maintains an overall risk assessment as part of its business-wide governance and management arrangements. As part of this risk assessment HCLTech identifies its Money Laundering risks and the

AML/CFT aspects of its risk assessments guide its policies, procedures and controls on a risk-based approach. This helps HCLTech identify and assess the risks which may or do impact its business and group, to then properly managed through policies, procedures and controls tailored to those risks.
HCLTech captures and records its risks in a Risk Register, as an additional component of its risk management policy, which includes Money Laundering risks. By identifying such risks, assessing their likelihood and impact, controls and additional controls for residual risks can be more effectively put in place.

5.4 KYC Principles

HCLTech conducts risk-based diligence on certain counterparties with whom it interacts to ensure, to a reasonable degree of confidence, that we know the parties with whom we do business and we have determined that the relationship would not violate the law or otherwise pose a risk to HCLTech's operations and/or reputation. Counterparties subject to risk-based due diligence may include customers, suppliers, vendors, subcontractors, consultants, distributors, agents, representatives and any other individual or entity with whom HCLTech enters into a contractual relationship in connection with the operation of HCLTech's global business. Due diligence is conducted in accordance with HCLTech's third-party management policies and due diligence procedures.
There may be circumstances where additional due diligence is required, beyond the standard due diligence requirements, for third parties who present a higher level of risk of money laundering or terrorist financing activities. For example, politically exposed persons, nationals or residents of high-risk jurisdictions and certain counterparty businesses or activities would trigger additional diligence requirements.

5.5 Transaction Monitoring

It is the responsibility of all HCLTech Personnel and Associates to alert the Compliance Department any time they observe or learn of conduct suggesting that a counterparty may be engaged in illicit activity.
Upon escalation to Compliance team of behavior by a counterparty that is indicative of potential illicit activity (e.g., negative news suggesting the counterparty's involvement in illegal activity, suspicious payment activity), Compliance team will work with the appropriate individuals who manage HCLTech's relationship with the counterparty, along with external counsel as appropriate, to determine an appropriate course of action. In circumstances where the counterparty at issue is not able to adequately explain the information or observed activity, an appropriate course of action could be to terminate HCLTech's relationship with the counterparty.
Where a specific payment has been identified, the individual who manages the relationship with the counterparty will work with Compliance team to obtain an explanation from the counterparty as to the business rationale for the payment at issue. If the counterparty cannot provide a business rationale for the payment, the counterparty will be instructed to cease such payment activity in the future in a circumstance where the payment has already been received into a HCLTech account. If HCLTech has not yet received the payment into a HCLTech account and a legitimate business rationale is not provided by the counterparty, HCLTech may refuse to accept the payment and direct the counterparty to make the payment in a more transparent way.
Under no circumstance will HCLTech accept a payment from, or make a payment to, a party where questions about the payment have arisen without an acceptable documented explanation from the counterparty as to the business purpose or rationale for the payment.

5.6 Avoid suspicious transactions:

Transactions which are suspicious in nature are to be completely avoided. All HCLTech Personnel and Associates should be aware of and watch for behavior patterns that are symptomatic of laundering situations. Some examples of such suspicious transactions or so called "red flags":

- Any reasonable person would suspect the transaction involves the proceeds of crime;
- The counterparty attempts to use unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's checks, or payments made in currencies other than those specified in the invoice;

o The counterparty is unwilling to provide complete or accurate information in response to HCLTech's due diligence inquiries, including but not limited to incomplete or inaccurate contact information, financial references, or business affiliations;
o The counterparty requests a deal structure unusual or unjustified complexity, with no apparent business or economic purpose;
o The counterparty exhibits unusual concern regarding HCLTech's compliance with this Policy, particularly with respect to its or his or her identity, type of business and assets; is reluctant or refuses to reveal any information concerning their business activities; or, furnishes unusual or suspicious identification or business documents;
o The counterparty wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the counterparty's stated business;
o The counterparty (or a person publicly associated with the counterparty) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
o The counterparty exhibits a lack of concern regarding risks, commissions, or other transaction costs;
o The counterparty appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity;
o The counterparty has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
o The counterparty requests overpayments or requests or attempts to make payments on an invoice(s) through multiple forms of payment or multiple parties;
o The counterparty requests funds owed to it by HCLTech be transmitted to an account other than the normal business relationship account or an account seeming unaffiliated with the counterparty; or
o The counterparty requests payments involving individuals or jurisdictions that have been deemed to be of money laundering concern by the U.S., U.K., or other government or international body (e.g., the Financial Action Task Force) or are considered restricted under U.S. or U.K. economic sanctions laws

6. Reporting

This Policy requires HCLTech Personnel and Associates to report any suspicions to **Global Ethics Helpline** as soon as practicable where they know or suspect that Money Laundering or Terrorist Financing activity is taking or has taken place, or if they become concerned that their involvement in a transaction brought by a counterparty may amount to a prohibited act under the applicable legislation. **Path:** MyHCLTech >>Top Ribbon (Main Menu)>> Ethics Helpline.

Employees based out of Germany/Netherlands shall continue to report any suspicions to whistleblower@hcltech.com as soon as practicable where they know or suspect that Money Laundering or Terrorist Financing activity is taking or has taken place, or if they become concerned that their involvement in a transaction brought by a counterparty may amount to a prohibited act under the applicable legislation.

If a question arises regarding this Policy, please contact the Compliance Department, or write to whistleblower@hcltech.com.

7. Training

HCLTech shall provide general AML training to its directors, officers, employees, and other personnel to ensure awareness of the requirements under this Policy. The training will include, at a minimum: how to identify red flags and signs of money laundering; what roles and responsibilities the directors, officers, employees and personnel have in HCLTech's compliance efforts, how to perform such duties and responsibilities and what to do once a red flag or suspicious activity is detected.

8. Violations and Disciplinary Actions

A violation of this Policy is a serious matter. Failure on the part of any HCLTech Personnel and Associates to follow this Policy could result in possible civil and criminal sanctions against HCLTech. Further this could result in possible disciplinary action against responsible individuals including and up to the person's

termination. Any violation of law or this Policy may also result in a loss of incentive compensation, bonuses, or other awards, to the extent permitted by law. HCLTech reserves the right to refer potential violations to regulatory and law enforcement authorities, if deemed appropriate under the circumstances.

9. References

This Policy should be read in conjunction with and interpreted alongside separate HCLTech documentation such as codes, policies, and procedures: below

- Code of Business Ethics and Conduct – Global
- Anti-Bribery and Anti-Corruption Policy – Global
- Trade Compliance/Sanctions Policy – Global
- Third Party Due Diligence Policy – Global
- Third Party Due Diligence Procedure – Global
- Corporate AML Compliance Programme – New Zealand

Annexure I - KYC

S No.	Particulars	Inputs
1.	Name of the Customer/Entity, Constitution of the Partner (Limited Corporation / Partnership / Individual)	
2.	Identification No. (In case of Individual – Passport Number / Local identification number and In case of entity / corporation, registration number / trade license allocated by the local registrar of companies or similar bodies)	
3.	Registered office address (with Zip Code / Postal Code, city and country) (In case of individual please give principal place of business only)	
4.	Principal place of business if different from registered office (with Zip Code / Postal Code, city and country)	
5.	Is your company is owned by another company, companies, persons or entities. (If yes, give the complete chain of shareholding up to the level of individual shareholder)	
6.	Telephone Number with country code	
7.	Facsimile Number with country code	
8.	URL of website if any	
9.	Official email address for correspondence	
10.	Single Point of contact	
	a) Telephone Number with country code	
	b) Facsimile Number with country code	
	c) Official email id for correspondence	
11.	Brief description of your services	
12.	Do you have any prior business relationship with HCLTech?	
13.	Does any of your employee or relative have any prior and existing relationship with HCLTech?	
14.	Are you involved in any litigation in past? (if yes, give details)	
15.	Describe data protection, privacy, confidentiality and intellectual property safeguards you take	
16.	Within the past five (5) years: Has your company or any related entity (e.g. parent or affiliate) or any of its, or their employees, board members, or officers been investigated, charged, or convicted in any jurisdiction, for engaging in any illegal activity related to unethical conduct, such as bribery or corruption?	
17.	Within the past five (5) years: Have you been investigated, charged, or convicted in any jurisdiction, for engaging in any illegal activity related to unethical conduct, such as bribery or corruption?	
18.	Banking Details:	

	a) Account Holder Name	
	b) Account Type	
	c) Full name of Bank	
	d) Address of Branch where account is held	
	e) Branch IFSC code	

KYC supporting documents

In case of an entity / corporation	In case of an Individual
1. Certificate of Incorporation or similar document issued by local registrar of companies or similar bodies 2. Certificate of good legal standing issued by some regulatory agency 3. If regulatory agency doesn't issue any such certificate of good legal standing then a declaration by a local law firm for good legal standing 4. Registration with local direct tax (Income Tax) authorities 5. VAT / GST registration certificate 6. List of Board of directors/Partners with their ID proofs (passport or local ID issued by Government bodies), email ID certified by Chairman of the Company 7. List of Shareholders certified by Chairman of the Company 8. Last 2 years audited financial certified by Chairman of the Company 9. Company Profile broadly covering nature of business	1. Certificate of good legal standing issued b some regulatory agency 2. If regulatory agency doesn't issue any suc certificate of good legal standing then declaration by a local law firm for good lega standing 3. Registration with local direct tax (Income Tax authorities 4. VAT / GST registration certificate 5. Latest CV of Individual duly signed Passpo Copy or any other local ID proof issued b Government bodies.