



Remedica

CUSTOMER AND VENDOR POLICY



1. INTRODUCTION

The purpose of this Customer and Vendor Policy (hereinafter referred to as the “Policy”) is to establish business acceptance procedures that ensure compliance of Remedica Limited (hereinafter referred to as the “Company” and together with its subsidiaries the “Group”) with all applicable legal requirements, and to identify, prevent or mitigate the risks to which the Group may be exposed during its business relationship with Customers and Vendors.

This Policy contains due diligence procedures designed to identify and evaluate the potential risks of working with a customer or vendor prior to and during the course of their business relationship with the Company. The identification and evaluation of customer and vendor risk is fundamental to the Company’s efforts to conduct business responsibly, sustainably and with integrity as set out in the Company’s Code of Ethics and Conduct. This includes preventing corruption and the use of the Group’s business to facilitate financial crime as well as ensuring integrity in the Company’s supply chain and compliance with sanctions laws and other legal requirements.

This Policy should be considered alongside the Group’s Anti-Bribery and Corruption Policy and Sanctions Policy.

All companies of the Group are obligated to meet the requirements of this Policy. They must also apply the highest standard of professional business conduct in any country where the Group conducts business and must operate in full compliance with the laws, rules and regulations applied to that country.

2. SCOPE

The Policy applies to any existing and potential business relationships of customers and vendors with members of the Group.

The term “vendor” as used in this Policy refers to those parties that manufacture, produce, assemble, sell, or otherwise supply products or services to the Group as well as those acting on behalf of the Group, such as commercial and other entities.

The term “customer” as used in this Policy refers to all parties to whom the Group supplies products and/or services, including but not limited to direct customers, distributors, agents and suppliers.

(Hereinafter referred to collectively as “Customers and Vendors” and individually as “Customer and Vendor”)

For this Policy to be effective, all employees and/or departments whose activities are directly associated with the engagement and/or communication with the vendors and/or customers, will undergo training aimed at providing a good understanding of the rules of this policy and how these affects them, the potential third party risks and an awareness of how the business may be used to facilitate financial crime.

3. RISKS

The Company considers that the employees that should undergo such training are from the Commercial Department (whose activities render adherence to the present Policy a requirement), the Accounting Department, the Corporate/Legal/Commercial Department, the Purchasing Department, the Sourcing Department, employees from the Engineering Department (whose activities render adherence to the present Policy a requirement), all Directors, Chiefs, Managers and Supervisors (hereinafter referred to collectively as the “Employees” and individually as the “Employee”).

Business relationships with customers and vendors expose the Company and the Group to financial, legal and reputational risks. It is important to understand these risks and set out how companies of the Group can identify any issues, concerns or constraints pertaining to these risks.

Any failure by the Company or the Group to comply with the applicable laws of the countries in which they operate may result in significant criminal, civil, and/or administrative penalties for both the Company and the Group and their involved employees. Non-compliance may also negatively affect the Company’s public image, reputation, share value, business opportunities, and market position.

Thus, the following risks (as applicable) must be understood and assessed in relation to all customer and vendor relationships of companies of the Group:

- ✓ non-compliance with applicable laws and regulations;
- ✓ adverse media related to unethical business practices or ongoing investigations;
- ✓ internal operational failures that may affect workflow efficiency;
- ✓ failure to deliver products as promised (e.g., quantity, quality and timing);
- ✓ poor financial health;
- ✓ operations in or dealings with high risk jurisdictions; and/or
- ✓ inadequate information technology resources.

4. RESPONSIBILITIES

The Compliance Team is responsible for the implementation of this Policy by all companies of the Group with the assistance of the affected Employees when requested by the Compliance Team. The Compliance Team is also responsible for reviewing and updating this Policy as and when required on (at least) a yearly basis.

Where an Affected Employee is in discussions with a new customer or vendor for the establishment of a business relationship is responsible for notifying the Compliance Team who will ensure that the checklist

included as Appendix I in the Policy is completed and approved before the Company or any company of the Group enters into an agreement with that customer or vendor. This checklist must be completed in accordance with the appropriate diligence process described in section 5 of this Policy considering the level of risk associated with that third party.

Upon the establishment of the business relationship, the Compliance Team, assisted by the Employee is responsible for the ongoing monitoring and due diligence of all existing customers and vendors, depending on their risk categorization. The ongoing monitoring procedure for LOW/MEDIUM risk vendors and customers shall be conducted every 3 years whereas for HIGH RISK vendors and customers on an annual basis. To permit effective ongoing monitoring and due diligence, the Employee must provide to the Compliance Team, all requested information and documentation.

4.1 When is Customer and Vendor Due Diligence required?

The due diligence in this Policy applies in addition to any credit/financial checks as may be required by the Company in respect of customers, vendors and/or other third parties. The Compliance Team shall maintain a current Approved Third-Party List of Vendors/Suppliers/Providers whom the Group has completed compliance on as to conduct business with. Prior to engaging with a vendor or customer the Employee has a duty to check first with the Compliance Team whether the said customer or vendor is included in the Approved Third-Party List.

Unless the third party appears on the Approved Third-Party List, due diligence must be conducted in the following circumstances:

- ✓ When establishing a new business relationship
- ✓ Where the reliability, accuracy or adequacy of documents, data or information previously obtained for the purpose of due diligence is doubted;
- ✓ In respect of a High party, a period of one year has passed since due diligence was last carried out on that third party, or;
- ✓ In respect of a third party connected with a Restricted Person, Entity, Organization, Government or Country. After due diligence is completed such a party will be monitored on an annual basis.
- ✓ If so directed by the Compliance Team or management of the Company.

If you become aware of any potential business relationship that may trigger the need to conduct enhanced due diligence on a customer or vendor as set out below in Section 5.5, you must notify the Compliance Team for guidance before entering into the business relationship (including the procurement of services, payment of invoices and similar activities).

4.2 Low Risk – Simplified Due Diligence

If no high-risk factors are identified as per section 5.5, the Compliance Team may proceed and apply simplified due diligence¹ on customers and vendors, so long as it has previously ensured that the business relationship or the transaction with them presents a lower degree of risk. Provided of course that the Compliance Team is carrying out sufficient monitoring of the said business relationship and transactions for the detection of any unusual or suspicious transactions.

When assessing the risks of money laundering, Sanctions or terrorist financing which relate to customers, countries or geographical areas, products, services, transactions or delivery channels the Compliance Team is obliged to take into account the factors of potentially lower risk situations which are as follows:

(1) Customer risk factors:

- ✓ companies listed on a stock exchange and subject to disclosure requirements, either by stock exchange rules or through law or enforceable means, which impose requirements to ensure adequate transparency of beneficial ownership;
- ✓ Public services or businesses;
- ✓ Customers with domicile in countries or geographical areas of lower risk as set out in paragraph (3);

(3) Geographical risk factors:

At the discretion of the Compliance Team, additional documentation relating to the customer or vendor may be required, such as e.g.:

- ✓ Company's KYC Questionnaires duly completed and signed by the vendor or customer.
- ✓ Corporate documents in case of an entity and the due diligence documents of its Ultimate Beneficial Owner and officers as listed in KYC checklist.
- ✓ Due diligence documents in case of individual vendor or customer as listed in the KYC Checklist.
- ✓ Power of Attorney in case of a person authorized to act on behalf of the Company.
- ✓ Additional screening of the third party's known directors, owners, and other beneficial owners (see Section 5.9).

¹ Simplified due diligence is the lowest level of due diligence that can be completed on a customer or vendor. This is considered appropriate where there is a little opportunity or risk of our services or customer or vendor becoming involved in money laundering or Sanctions.

5.4 Medium Risk – Standard Due Diligence

If the simplified due diligence procedure described above does not apply, and no high-risk factors are identified as per section 5.5 the Compliance Team may proceed and apply the standard due diligence on customers and vendors

The standard due diligence involves identifying your customer and verifying its identity.

This means that the Compliance Team will need to be provided with the following:

- ✓ Company's KYC Questionnaires duly completed and signed by the vendor or customer.
- ✓ Corporate documents in case of an entity and the due diligence documents of its Ultimate Beneficial Owner and officers as listed in KYC checklist.
- ✓ Due diligence documents in case of individual vendor or customer as listed in the KYC Checklist.
- ✓ Power of Attorney in case of a person authorized to act on behalf of the Company.
- ✓ Minutes of Approval of Signatory by the Board of Director in case of a person authorized to sign on behalf of the Company.
- ✓ Financial statements (if establishing a trading relationship);

The Model Clauses included as Appendix II in the Anti-Bribery & Corruption Policy, the applicable version for Third Parties and Intermediaries (such as Agents and Distributors) and Customers must be included in the agreement.

5.5 High Risk – Enhanced Due Diligence

Enhanced due diligence must be applied if any of the customer or vendor, agent(s), service providers, freight forwarder, carrier, delivery address, bank(s) or payer is located in or in transit with a High-Risk Country for:

Corruption: These are countries of higher risk of bribery and corruption which have a score of less than 50 in the Corruption Perception Index published by Transparency International², or;

Tax evasion: These are countries included in the EU list of non-cooperative jurisdictions³, or;

² See: <https://www.transparency.org/en/cpi/2020/index/nzl>

³ See: <https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/#>



Money Laundering and Illicit Drugs risks: these are countries subject to the Financial Action Task Force monitoring in respect of deficiencies in their anti-money laundering laws⁴ and countries designated by the U.S. State Department for high risk related to illicit drugs⁵.

If the business relationship is assessed as High Risk, the following documentation relating to any third party that is a corporate entity is required:

- ✓ Company's KYC Questionnaires duly completed and signed by the vendor or customer.
- ✓ Corporate documents in case of an entity and the due diligence documents of its Ultimate Beneficial Owner and officers as listed in KYC checklist.
- ✓ Due diligence documents in case of individual vendor or customer as listed in the KYC Checklist.
- ✓ Power of Attorney in case of a person authorized to act on behalf of the Company.
- ✓ Minutes of Approval of Signatory by the Board of Director in case of a person authorized to sign on behalf of the Company.
- ✓ Financial statements (if establishing a trading relationship);

The Compliance Team upon receipt of all the above documents shall conduct sanctions' screening procedure as per section 5.9 to ensure that the Company will not engage in any business involving Restricted Parties.

In case a Restricted Party is identified then the Employee must first obtain the approval of the Compliance Team prior engaging with same.

The Anti-Bribery & Corruption Model Clauses, the applicable version for Third Parties and Intermediaries (such as Agents and Distributors) and Customers incorporated as Appendix II in the Anti-Bribery & Corruption Policy must be included in the agreement.

5.6 Very High Risk – Enhanced Due Diligence and Sanctions Compliance

Enhanced due diligence and sanctions compliance measures are to be applied if any of the customers, vendors, service providers, agent(s), freight forwarders, carriers, delivery addresses, bank(s) or payer is located in or a transit country is a “**Sanctions List Country**”.

⁴ See: <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html>

⁵ See: <https://www.state.gov/presidential-determination-on-major-drug-transit-or-major-illicit-drug-producing-countries-majors-list/>



5.7 Comprehensively Sanctioned Country – Enhanced Due Diligence and Sanctions Compliance

Enhanced due diligence and sanctions compliance measures are to be applied if any of the customer or vendor, service providers, agent(s), freight forwarder, carrier, delivery address, bank(s) or payer is located in or a transit country is a country or territory currently subject to U.S. comprehensive sanctions.

Reference must be made to the Sanctions Policy, paragraph 8.5 for the due diligence and the agreement clauses that must be included in the agreement with the customer or vendor.

5.8 For each new and existing business relationship the Compliance Team will to complete the form at Appendix I and include all relevant documents. Such form shall only be completed upon completion of the due diligence procedure on the new business relationship and upon completion of the ongoing monitoring on existing business relationship. All affected Employees shall only proceed and engage with the customer/vendor upon receiving first the approval from the Compliance Team.

This paragraph applies to all level of risks mentioned above.

5.9 Sanctions Screening

Effective screening measures are essential to the management of sanctions risks and to ensure that the Company does not engage in any business involving Restricted Parties.

The Customer & Vendor Policy must be followed in order to ensure such screening is executed for all customers and vendors. All affected Employees are obligated to aid, when requested by the Compliance Team, for the collection of all relevant information and documentation on parties the Company transacts with in order to enable the screening of these business partners.

The sanctions' screening procedure is operated by the Compliance Team via LSEG World-Check One. LSEG World-Check One is a database of Politically Exposed Persons (PEPs) and heightened risk individuals and organizations, used around the world to help to identify and manage financial, regulatory, and reputational risk.

The Compliance Team will conduct screening for all Third Parties as required under this Policy. Furthermore, the Customer & Vendor Policy must be followed to ensure such screening is executed as well for all customers and vendors. In particular, it is essential for all relevant information on parties the Company transacts with to be forwarded to the Compliance Team to enable the screening of these business partners.

During the screening procedure the Compliance Team checks the names of third parties, their directors and beneficial owners against Sanctions Lists to determine whether or not there is a potential sanctions' match. If the screening reveals such a potential match, the Compliance Team will determine whether there is an actual match, in which case the contemplated transaction will be prohibited, or whether the potential match is a false positive.



The sanctions screening will occur prior to commencing a new business relationship as well as periodically for existing business relationships to ensure ongoing sanctions compliance. Any potential hits from the periodical automated screening are reviewed by the Compliance Team for evaluation.

5. ONGOING MONITORING ON EXISTING CUSTOMERS/VENDORS

Continuous monitoring is the process that entities take to ensure that their business relationships are consistent in order to keep their information about their customers and vendors up-to-date and the transactions of same are performed as expected of them.

When conducting ongoing monitoring on existing customers or vendors, the Compliance Team, with the assistance of the affected Employees as this may be requested by the Compliance Team, should check that all information initially provided by the customer or vendor is the same and in case of change new, updated documents to be requested by the Customer or Vendor.

In case it comes to the attention of an Employee of a suspicious transaction then the Compliance Team must be informed immediately in order to investigate the matter further.

6. PAYMENTS

Controls must be in place to ensure that payments are made to and from accounts opened in the name of the customer or vendor in the country of its business operations. All affected Employees should not without the prior approval of the Compliance Team make or agree to receive any payment to or from an account;

- ✓ which does not match the name of the third party; or
- ✓ is in a country in which the Third Party is neither registered nor conducts business.

7. RECORDS

7.1 The Compliance Team shall maintain for each new and existing Customer and Vendor documents and information for a period of five (5) years following the termination of the business relationship.

7.2 The Compliance Team must update the Approved Third Party List on a per annum basis, and in any case, when a third party is approved, if already approved or loses its approval status.

8. CONTRACTS

Every engagement with a customer or vendor that requires due diligence under this Policy must be accompanied by a contract in writing that, at a minimum, contains:

- ✓ the products and/or services to be provided by the vendor;
- ✓ the price or compensation payable by the Company;



- ✓ a statement of adherence by the vendor to the Code of Ethics and Conduct, either as set out in Appendix II and III, or via e-mail confirmation, or, through the adoption of equivalent principles by the vendor by its own codes and/or policies;

Should any complication arise in connection with the contractual relationship with any Customer or Vendor then the Company will be able to deviate from the present Policy only with the prior approval of the Audit Regulatory Committee (hereinafter referred to as the “ARC Committee”).

9. QUESTIONS AND DISTRIBUTIONS

Any questions, concerns, or suggestions regarding this Policy should be addressed to the Compliance Team.

Copies of this Policy shall be distributed to all affected Employees, Customers and Vendors.

Head of Legal And Compliance Department: Elina Skoullou

Contact Number: (+357) 25 553 584

Email Address: E.Skoullou@remedica.eu

ComplianceRem@remedica.com.cy

APPENDIX I:

CUSTOMER AND VENDOR DUE DILIGENCE CHECKLIST AND SIGN OFF

Name of Company/Individual:	
Country of Incorporation/Residence:	
Reason for KYC (New Customer or Vendor business relationship or Existing Customer or Vendor business relationship please specify)	
Risk Category (Low, Medium, High, Very High, Restricted (Customer NGO), Restricted (without NGO)):	
Confirm all relevant documents obtained for all involved: A. KYC documents of Customer or Vendor (entity or individual). B. KYC documents of other involved parties such as agent(s), freight forwarder, carrier, delivery address, bank(s) or payer (entity or individual).	
Approved by: (signature of [x])	
Date of Approval:	
(signature of [x])	
Date of 2nd Level Approval:	
Date of Next Review: (1 year if high risk (or higher); 3 years in all other cases)	



APPENDIX II:
REMEDICA HOLDINGS LIMITED
(“The Company”)

CUSTOMER/VENDOR STATEMENT OF ADHERENCE

Natural Person

I _____ holder of passport/ID no _____ acting as _____ (*customer or vendor*) hereby state and confirm that I have reviewed and understood the Company’s Customer and Vendor Policy and agree throughout my business relationship with the Company, to comply with the requirements set out in this Policy.

Name:

Date:

Signature:



APPENDIX III:
REMEDICA HOLDINGS LIMITED
(“The Company”)

CUSTOMER/VENDOR STATEMENT OF ADHERENCE

Legal Entities

We _____ with registration no. _____ and registered office address at _____ acting as _____ (*customer or vendor*) hereby state and confirm that we have reviewed and understood the Company’s Customer and Vendor Policy and agree throughout the duration of our business relationship with the Company to comply with the requirements set out in this Policy.

Company Name:

Name of the Authorised Signatory:

Title of the Authorised Signatory:

Signature: