THIRD PARTY DUE DILIGENCE POLICY

1. Introduction

RA (or "Company") is committed to doing business with integrity and in full compliance with applicable laws and international best practices. The Company's aim is to maintain a best-in-class governance and compliance environment. This is not only a source of competitive advantage but also expected by our stakeholders.

Everyday RA contracts with third parties to provide the Company with goods and services. RA is aware that it may be held liable for acts of corruption by any individual or entity that has some form of business relationship with RA.

RA has zero tolerance to bribery and corruption and only conducts business with third parties that share similar values and ethical standards. Given that RA International Group is listed on the London Stock Exchange and the nature of RA's clients (United Nations, US and UK Governments, large multinationals, etc.), transacting with third parties who are sanctioned or flagged by international bodes could be especially damaging to the Company and could lead to significant financial, operational, or criminal penalties against both the Company and/or its employees and directors.

In order to consistently maintain ethical standards across the organization, RA has defined a risk-based process to conduct due diligence on third parties with which it conducts business.

This Policy should be read in conjunction with RA Code of Conduct and Anti-Bribery Corruption Policy.

2. Definitions

- **Business Sponsor:** is the delegated person in RA making the request to appoint a third party.
- **Third Party:** for purposes of this Policy, the term "Third Party" includes but is not limited to contractors and subcontractors (suppliers of goods and services), consortium partners, consultants, distributors, sales agents, dealers, joint venture partners, and any other third party acting for or on behalf of RA:

  - **Agent**

  An individual or organization authorized to act for or on behalf of, or to otherwise represent, another organization in furtherance of its business interests. Agents may be categorized into the following two types: - Sales agents (i.e. those needed to win a contract) - Process agents (e.g. visa permit or customs clearing agents).

  - **Contractor and Sub-contractor**

  A contractor is a non-controlled individual or organization that provides goods or services to an organization under a contract.

  A subcontractor is an individual or organization that is hired by a contractor to perform a specific task as part of the overall project.

  - **Consortium Partner**

An individual or organization which is pooling its resources with another organization (and possibly other parties) for achieving a common goal. In a consortium, each participant retains its separate legal status.

- **Customer**

The recipient of a product, service or idea purchased from an organization. Customers are generally categorized into two types: - An intermediate customer is a dealer that purchases goods for resale. - An ultimate customer is one who does not in turn resell the goods purchased but is the end user.

- **Consultant**

Any person who is engaged by the Company or any Related Entity to render consulting or advisory services to the Company or such Related Entity but is not employed by the company.

- **Joint Venture Partner**

An individual or organization which has entered into a business agreement with another individual or organization (and possibly other parties) to establish a new business entity and to manage its assets.

- **Supplier/Vendor**

An individual or organization that supplies parts or services to another organization.

- **Service Provider**

An individual or organization that provides another organization with functional support (e.g., communications, logistics, storage, processing services).

- **Red Flag** is a term used to identify a fact which requires further information to assess.

3. Relevant Regulatory Standards

This Policy is aimed at ensuring that the engagement procedures for Third Parties incorporate the key requirements of legislation such as the UK Bribery Act (UKBA) and the US Foreign Corrupt Practices Act (FCPA), which may be applicable to RA entities and/or operations.

US Foreign Corrupt Practices Act 1977 (FCPA) - Under the FCPA, an organization or individual may be held liable for making payment to a third party while knowing that all or a portion of the payment will go directly or indirectly to a foreign official. To avoid being held liable for corrupt third-party payments, the US Department of Justice encourages companies to "exercise due diligence and to take all necessary precautions to ensure that they have formed a business relationship with reputable and qualified partners and representatives".

The UK Bribery Act 2010 - In its Adequate Procedures Guidance to the UK Bribery Act, the UK Ministry of Justice states that "a commercial organization will be liable to prosecution if a person associated with it bribes another person intending to obtain or retain business or an advantage in the conduct of business for that organization". An "associated person" is defined as an individual or entity that "perform services for or on behalf" of an organization. In the event of failure to prevent bribery by an associated person, the UK Bribery Act provides that is a "defense" for an organization "to prove that (it) had in place adequate procedures designed to prevent people associated with (it) from undertaking such conduct".

4. Scope

This Policy is applicable to the selection, appointment, and on-going management of third parties engaged by RA in furtherance of its global business aims.

The Scope may also be extended to internal stakeholders like RA employees and/or temporary contractual staff such as consultants.

Where it is not clear whether a proposed relationship between RA and another party falls under this Policy, advice should be obtained from RA Compliance before making any written or verbal commitment regarding any potential relationship.

Governmental customers, UN agencies and international NGOs are not in scope of this Policy.

5. Purpose

The purpose of the third-party due diligence policy is to help prevent and limit the exposure of RA to any act of bribery and corruption and to prevent RA entering into a business relationship with a sanctioned entity. Accordingly, before engaging any third party this Policy must be followed.

6. Roles and Responsibilities

6.1 COMPLIANCE MANAGER

The Compliance Manager is responsible for overseeing and administering the due diligence process and is responsible for reviewing and analyzing information provided by a Third Party, the Business Sponsor and any other relevant party.

The Compliance Manager coordinates with Operational Departments and request additional information or documents from a prospective Third Party, as necessary.

The Compliance Manager will identify the appropriate level of due diligence by assessing the risk level (utilizing Third Party Review Criteria) and the presence of any Red Flags, as defined herein. If deemed necessary under the appropriate level of due diligence, the Compliance Manager may coordinate with the Business Sponsor to provide and collect a Third-Party Due Diligence Questionnaire, customized, if necessary, to reflect unique circumstances, from the Third Party.

The Compliance Manager will have responsibility for final approval, rejection, or requests for further information from a Third Party.

6.2 BUSINESS SPONSOR

The Business Sponsor is responsible for coordinating with the Compliance Manager to meet the requirements of this Policy.

If requested by the Compliance Manager, the Business Sponsor will provide a statement of the business case for a relationship with a Third Party, including details such as business need, reasonableness of proposed compensation and comparison with the market, capabilities of the proposed Third Party, reason for selection, and description of the relationship formed to date.

The Business Sponsor will also be responsible for distributing and collecting the Third-Party Due Diligence Questionnaire, or any other applicable form, and relevant support documents to/from the potential Third Party to obtain the information necessary to conduct a thorough due diligence review.

6.3 OPERATIONAL DEPARTMENTS

Operational Departments, such as Procurement, Logistic, Finance, PM, BID, and/or others, are responsible for supporting the Compliance Manager's administration of the due diligence process. This may include, as necessary, implementing policies and operating procedures to ensure that the due diligence process is followed.

7. Due Diligence Process

7.1 THIRD-PARTY RISK ASSESSMENT

RA assesses third parties as high, medium, or low-risk. The level of risk will ultimately determine the amount of due diligence that RA believes is required, with high-risk third parties subject to a more detailed due diligence process.

7.2 KEY RISK INDICATORS:

- Corruption Perception Index (CPI)
- Geographical Location
- Background and identity of Third-Party Connection with Government officials or entities
- Additional factors related to the scope of the services to be rendered

Following categorization of Third Parties, the appropriate levels of due diligence must then commence.

Low-risk third parties are those located in a country with a CPI score of 50 or above. In this case, the process will consist of Internet searches, database and company documents checks.

Medium- to high-risk third parties are those located in a country with a CPI score below 50. In this case more thorough data collection will take place and the process will consist of a full reputational screening which includes:

(i) checking for updates to sanctions/watch lists;

(ii) checking for updates to Politically Exposed Persons (PEP) lists; and

(iii) checks for exposure to global adverse media.

RA is implementing an automated system to perform the third-party screening (RiskRate by NAVEX Global). This will allow RA to enhance its risk-based approach through the use of third-party risk management and due diligence strategies.

RA recognizes the three key elements to conducting a thorough third-party due diligence to be:

- Data collection
- Verification and validation of data
- Evaluation of results, including identification of red flags

Once data has been properly verified and validated, RA will determine whether or not to move forward with the proposed third-party business relationship. To assist with this judgment, collected data will be tested against a "Red Flag" Checklist.

A detailed Red Flag Checklist is attached as Appendix 1.

8. Due Diligence Frequency

The due diligence process is required to be repeated at regular intervals including, but not limited to:

- Contract renewal;
- Significant amendment to contract (e.g. nature of transaction/scope of services/amount of remuneration);
- Change of control as communicated by the third party or change identified during the annual due diligence process in third party(ies); and
- Every two years for low-risk parties; and every year for high-risk parties.

In addition to repeating the due diligence process as at the above dates, RiskRate will monitor third-parties and will update the Company if Red Flags or changes in risk rating occur.

9. Contractual Provisions

RA Terms and Conditions include provisions to mitigate potential corruption or bribery risk

Additional anticorruption provisions may be added to contracts with any Third Party to mitigate risks identified during the Due Diligence Process, such as: anticorruption representations and warranties, specific risk-based certifications to confirm representations made during the Due Diligence review, audit rights, termination rights, payment terms, and additional provisions which may be required based on the specific circumstances.

Any additional contract terms must be approved by the Legal Department, in consultation with the Compliance Manager.

10. Disqualification of Third Party(ies)

A third party may be blacklisted in cases including, but not limited to:

a) Non-compliance with RA's Code of Conduct and Anti-bribery Corruption policies and procedures.

b) Infringement of ethical standards in business dealings.

11. Monitoring, Training and Review

Following any agreement of a business relationship with third parties, the third party will be monitored in the following ways:

a) Constant monitoring of the risk assessment and any red flags through RiskRate

b) Recurring Internet and database searches to identify new red flags

c) Implementing a post-approval assurance program, including training activities and periodic and/or risk-based audits of the third party

d) Annual certification of compliance with applicable anti-corruption laws

e) A periodic review of the third party's payment requests and payments

f) Tracking unusual or excessive expenses by the third party

Training will be used to communicate RA's anti-corruption standards and procedures to personnel. Training content and method will be tailored to employee responsibilities. Decisions regarding when and in what form to offer training support should reflect the third party's risk profile and the degree of corruption risk in the relationship.

The Compliance Manager together with RA senior management will monitor the third-party due diligence process, periodically review its suitability, adequacy and effectiveness, and implement improvements where needed.

Spot checks may be used to ensure that the due diligence process is properly applied and to deter any potential abuse. The organization will endeavor to regularly reassess due diligence measures ensuring they are adapted.

12. Records

RA Compliance Manager will centrally maintain records relating to the Third Parties due diligence. The document(s) shall be readily made available for reference as required.

Soraya Narfeldt

CEO

Policy Implementation/ Review Date	Next Policy Review Date
January-2026	January-2027

APPENDIX 1 - POTENTIAL RISK SCENARIOS: "RED FLAGS"

1. The following is a list of possible red flags that may arise during the course of any representative working for or on behalf of RA, and which may raise concerns under various anti-bribery & corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only. If you encounter any of these red flags you must promptly report them to the Compliance Manager or, alternatively, via the Company's confidential reporting processes outlined in its Code of Conduct and its Whistle Blower Policy:

   1.1 you become aware that a Third Party has a poor reputation and/or engages in, or has been accused of engaging in, improper business practices;

   1.2 you learn that a Third Party has a reputation for paying bribes, or requiring that bribes are paid to them;

   1.3 a Third Party:

      1.3.1 insists on receiving a commission or fee payment before committing to sign a contract with the Company, or carrying out a government function or process for the Company;

      1.3.2 requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

      1.3.3 requests that payment is made to a country or geographic location different from where the Third Party resides or conducts business;

      1.3.4 requests an unexpected additional fee or commission to "facilitate" a service;

      1.3.5 demands lavish entertainment or gifts before commencing or continuing negotiations or discussions on a matter;

      1.3.6 requests that a payment is made to "overlook" potential legal violations;

      1.3.7 requests that you provide employment or some other advantage to a friend or relative;

      1.3.8 requests that you enter into a contract; or

      1.3.9 has unexplained preferences for certain sub-contractors;

   1.4 you learn that a colleague has been taking out a particular government official for very expensive and frequent meals;

   1.5 you receive an invoice from a Third Party that appears to be non-standard or customised;

   1.6 you notice that the Company has been invoiced for a commission or fee payment that appears large or small given the service stated to have been provided;

   1.7 you notice the establishment of unusual or unexplained bank accounts or funds;

   1.8 the country in question is known for bribery or there have been regular media reports of bribery in such country; or

   1.9 a Third Party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to the Company.