2023

THIRD PARTY COMPLIANCE MANAGEMENT POLICY

RABIGH REFINING AND PETROCHEMICAL COMPANY

(Petro Rabigh)

Title: Third Party Compliance Management Policy		
Policy Reference:		
Applicable to: Directors, Executive Management, Officers, and Employees; Third Party Representatives		
Replaces	**Effective Date**	**Pages**
N/A	**[●]** 2023	7

1. Introduction and Purpose

1.1. The Company enters into business relationships with a variety of Third Parties to perform services and provide products for or on its behalf. The Company recognizes that the engagement of Third Parties poses certain financial and reputational risks to the Company and the Company is committed to effectively manage such risk. In furtherance of that commitment, the Company has adopted this Global Third Party Compliance Management Policy (the "Policy"). This Policy provides a framework for the Company to appropriately assess, measure, monitor, control and report the risks associated with the Third Party relationship. The Company recognizes that it cannot eliminate all risk posed by the engagement of Third Parties but strives to identify and mitigate such risks through effective compliance management.

1.2. It is the policy of the Company to comply with all laws governing our operations wherever the Company does business, including safety standards and regulations; all applicable anti-corruption laws; laws and regulations governing economic sanctions and export controls; and laws prohibiting money laundering or terrorist financing. The Company expects Third Parties performing services for the Company or interacting with others on the Company's behalf to abide by all applicable laws and regulations. Additionally, Representatives (as defined below) acting on behalf of the Company are subject to the same compliance restrictions as Company employees.

1.3. This Policy shall be adopted by a resolution of the Board of Directors ("Board"), following a recommendation by the Audit Committee, and shall enter into effect from the date on which it is approved by the Board.

1.4. The Audit Committee shall periodically review the provisions of this Policy and recommend any amendments thereto to the Board.

1.5. Any amendments to this Policy shall be adopted in the same manner in which this Policy was adopted.

2. Policy Scope

2.1. This Policy applies to business arrangements between a Third Party and the Company by contract or otherwise, to perform services and provide products for or on the Company's behalf. This Policy also covers all directors, Senior Management, and employees of the Company (including any senior executives and employees on secondment from other entities) (collectively, "**Company Personnel**").

3. Definitions

3.1. **"Business Relationship Owner ("BRO")** means the business line or product line manager (or other Company Personnel as designated by the head of the respective business unit) who is primarily responsible for managing the relationship with a Third Party.

3.2. **"Inherent Risk"** means the intrinsic risk prior to considering any controls in place.

3.3. **"Risk Assessment"** means the overall process of risk identification, risk analysis and risk evaluation for Third Party Representatives.

3.4. **"Risk Tolerance"** means the level of risk that the Company is willing to accept in pursuit of strategic goals and objectives.

3.5. "**Senior Management**" means persons responsible for managing the daily operations of the Company, and proposing and executing strategic decisions, including the President and CEO, his deputies, the CFO, and the CCO.

3.6. "**Third Party"** means any entity or person not under the direct business control of the Company with whom the Company engages in a business relationship, including any vendor, supplier, support provider, fulfilment provider, consultant, advisor, or strategic partner. A Third Party may also act as a Representative of the Company, as defined below. Third Parties do not include Company Personnel, investors, or customers.

3.7. **"Representative"** means any outside Third Party individual or organization that is retained to represent or act as an agent or otherwise on behalf of the Company to assist in securing a contract or other business advantage in any context, including in connection with the sale of the Company's goods or inspections, customs, import/export, permitting, shipping, or regulatory matters. Representatives may include, among others, agents, brokers, marketers, and distributors.

3.8. **"Third Party Risk Management ("TPRM")** means the Company's formalized program of identifying, assessing, and mitigating risks to the Company and Company Personnel, investors, and customers due to the improper supervision or mismanagement of the following: data, operations, compliance, and financial conditions concerning those external parties with whom the Company has a relationship. Third Party Risk Management is also inclusive of all reporting, governance, and oversight activities necessary to ensure sound engagement with the Company's Third Parties.

4. Pre-Existing Third Party Relationships

4.1. It is the goal of Senior Management and the Board to comply with this Policy with respect to Third Party relationships maintained with the Company. The Board recognizes that certain existing Third Party relationships (and contracts) may not comply with all aspects of this Policy. It is Senior Management's responsibility to continuously seek opportunities to renegotiate changes (e.g., at contract renewal, etc.) to existing Third Party contracts in order to achieve full compliance with this Policy.

5. Risk Management Process

5.1. **In General.** To effectively use a Third Party in any capacity, the Company must appropriately assess, measure, monitor, control and report the risks associated with the relationship. While engaging another entity may assist management in achieving strategic goals, such an arrangement reduces management's direct control and may heighten certain risks. Therefore, the use of a Third Party increases the need for a documented risk management process.

5.2. **Elements of TPRM.** In accordance with sound Companying practices and in keeping with applicable supervisory guidance, the following four elements shall be addressed in the Company's TPRM Program:

- Assessment of risk and related documentation;
- Risk-based due diligence and selection of service providers;
- Contract provisions, considerations, and maintenance; and
- Oversight and monitoring of Third Parties.

While these four elements apply to any Third Party activities, the precise scope of the process with any particular Third Party will be dependent on numerous factors such as the nature of the Third Party relationship, the scope and magnitude of the activity, and the specific risks identified.

6. Assessing Risks Posed by Third Parties

6.1. **In General.** There are numerous risks that may arise from the Company's use of Third Parties. Some of the risks are associated with the underlying activity itself, similar to the risks faced if the Company conducted the activity. Other potential risks arise from or are heightened by the involvement of a Third Party. Failure to manage these risks can expose the Company to regulatory action, financial loss, litigation and damage to the Company, and may even impair the Company's ability to establish new or service existing customer relationships.

6.2. **Specific risks.** In general, the TPRM shall require an assessment of the following risks as appropriate under the circumstances:

- **Strategic Risk.** Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the Company's stated strategic goals. The use of a Third Party to perform Company functions or to offer products or services that do not help the Company achieve corporate strategic goals and provide an adequate return on investment exposes the Company to strategic risk.

- **Reputation Risk.** Reputation risk is the risk arising from negative public opinion. Third Party relationships that result in dissatisfied counterparties, interactions not consistent with Company policies, inappropriate recommendations, security breaches resulting in the disclosure of confidential information, and violations of law and regulation are all events that could harm the reputation and standing of the Company. Also, any negative publicity involving the Third Party's practices, whether or not the publicity is related to the Company's use of the Third Party, could result in reputation risk.

- **Operational Risk.** Operational Risk is the risk of a Third Party causing disruption to the Company's business operations arising from problems with service or product delivery. A Third Party's failure to perform as expected due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes the Company to Operational risk. The lack of an effective business resumption plan and appropriate contingency plans increase Operational risk.

- **Cybersecurity Risk.** Cybersecurity risk is the risk of exposure or loss resulting from a cyberattack, security breach, or other security incidents with a Third Party that could compromise Company data.

- **Compliance Risk.** Compliance risk is the risk arising from violations of laws, rules, or regulations, or from intentional or inadvertent non-compliance with internal policies or procedures or with the Company's business standards. This risk exists when the activities of a Third Party are not consistent with governing laws, rules, regulations, policies, or ethical standards. Liability could potentially extend to the Company when Third Parties violate laws, rules, regulations, or other required practices. Compliance risk is exacerbated when an entity has inadequate policies, oversight, monitoring or audit functions.

- **Other Risks.** The types of risk introduced by the Company's decision to use a Third Party cannot be fully assessed without a complete understanding of the resulting arrangement. Therefore, a comprehensive list of potential risks that could be associated with a Third Party relationship is not possible.

6.3. **Responsibilities of Business Relationship Owner.** The head of each business unit shall designate a BRO who is primarily responsible for managing the relationship with a Third-Party. The BRO shall

be the first line of defense for ensuring compliance by identifying risks and escalating significant matters of concern to the head of the respective business unit.

6.4. **Risk Metrics and Tolerance.** Each business unit of the Company shall identify risk metrics and risk tolerances subject to the approval of the Company's Chief Compliance Officer ("**CCO**") and consistent with any Board-approved risk tolerance statement applicable to Third Party risk. Additionally, Senior Management and the Board must be kept regularly informed of any material issues related to the Company's Third Party relationships and the diligence, contract negotiation and monitoring of all critical Third Party relationships.[1]

7. Risk Assessment and Process

7.1. **Risk Assessment.** Each prospective Third Party relationship will be assessed by the head of the respective business unit for the inherent risk posed to the Company based on the criticality of the products/services provided and the manner in which they are provided. The risk rating should be used to determine the scope and depth of the due diligence performed, documentation requirements, contractual terms and conditions, the scope, of monitoring and risk re-assessments, and the transition process for off-boarding.

7.2. **Specific Risk Areas.** Specific risk areas that may be examined to assess risk include:

- Business Continuity Risk
- Compliance Risk
- Financial Risk
- Legal Risk
- Cyber Risk
- Country Risk
- Transactional Risk
- Concentration Risk
- Information Security Risk
- Privacy Risk
- Strategic Risk
- Operational Risk
- Reputational Risk

7.3. **Risk Ratings**. Low, Moderate, and High ratings are assigned to Third Party engagements. The Risk Rating shall be assigned by the head of each of the respective business unit or appropriate designee.

7.3.1. Low

- The relationship's nature and the Third Party's risk profile present little-to-no risk, and minimal ongoing monitoring is warranted.
- The Third Party has minimal or no access to or interaction with customers or confidential employee, investor, or customer information.
- Third Parties that provide services incidental to the Company's operations or for which the Company would have readily available an acceptable alternative vendor or an adequate, alternative means to provide those contracted services while operating at acceptable levels of service with little or no risk of financial loss.

[1] A Third Party is considered critical when performing an activity deemed crucial to the Company's operations or is the sole provider of an essential business function.

7.3.2. Moderate

- The nature of the relationship (such as a Representative acting on behalf of the Company) or the Third Party's risk profile presents some level of risk, and periodic oversight is necessary.
- The Third Party has limited access to or interaction with customers or confidential customer information.
- Third Parties that perform a useful function but provide services that could be easily replaced by another vendor to minimize disruption to the Company's operations or customers and ensure continuity of operations.

7.3.3. High

- The nature of the relationship and the Third Party's risk profile present a significant risk that must be mitigated and requires frequent oversight through due diligence and monitoring activity.
- Third Parties that provide services or products critical to the Company's daily operations.
- Representatives who are interacting with government officials on behalf of the Company.
- Notwithstanding any other risk factors presented, any Third Party with regular access or interaction with customers and confidential customer information
- Third Parties who provide services in countries subject to KSA, UN, EU, or US sanctions.

7.4. Unless otherwise authorized by the CCO or exempt as a "Routine Vendor,"[2] all new Third Party engagements or expansion of existing relationships must have an Inherent Risk Rating. Company Personnel shall use the Third Party Decision Tree and Third Party Procedures that implement this policy to determine the nature and extent of each Third Party's risks.

8. Due Diligence

8.1. **In General.** Upon completion of a Third Party Risk Assessment, risk-based due diligence tailored to the specific needs and standards of the applicable business unit and the unique factors presented by the pending relationship must be undertaken. The due diligence process shall be appropriately scaled in order to provide Senior Management with the information needed to address qualitative and quantitative aspects of potential Third Parties to determine if a relationship would help achieve the Company's strategic and financial goals and mitigate identified risks.

8.2. **Timing.** Not only should due diligence be performed prior to selecting a Third Party, but it should also be performed periodically during the course of the relationship, particularly when considering the renewal of a contract.

8.3. **Scope.** Due diligence involves a review of relevant information about a potential Third Party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls. The scope and depth of due diligence will be tailored to the importance and magnitude of the Company's

[2] A "Routine Vendor" is a supplier or vendor that provides a standard good or service generally available to the public and not specific to the Company, and that is not a Representative. Routine Vendors might include, for example, providers of office cleaning or repairs and maintenance services, sellers of office supplies, and insurance carriers. Routine Vendors are generally exempt from the requirement to prepare a Risk Rating. Any contract with a routine vendor, however, should still be in writing and allow for termination for a crime or violation of applicable anti-bribery/anti-corruption laws.

relationship with the Third Party and the risks associated with the Third Party relationship. Additional business-unit or product specific standards may be included as appropriate or as identified risks may dictate (such as for Third Parties located in high risk jurisdictions).

9. Contractual Standards

9.1. **In General.** All Third Party relationships are required to be documented pursuant to a written agreement that adequately addresses the contemplated relationship and provides the Company with appropriate protections and controls, consistent with prudent business practices.

9.2. **Contract Terms and Provisions**. Contracts with Third Parties should adhere to the same general guidelines as other contractual relationships in which the Company is involved. Agreements with Third Party Representatives shall (i) be in writing, (ii) specifically describe the services to be performed, (iii) allow the Company to terminate the agreements in the event of a Third Party Representative's commission of a crime or violation of applicable anti-corruption or anti-bribery laws, sanctions, or trade controls, (iv) require Third Party Representatives to represent and covenant compliance with applicable laws, including anti-corruption laws, and (v) contain other provisions as may be set forth in procedures promulgated by the Company. The level of detail in contract provisions may vary with the scope and risks associated with the Third Party relationship.

9.3. **Procedures for Review and Execution.** The Company shall establish procedures for contract review and approval prior to execution, and shall set appropriate risk-based thresholds, for levels of review and approval. The Program shall further establish contract signature authority for each business unit or functional area of the Company.

9.4. **Contract Management.** Contract renewal dates and/or termination dates shall be actively managed and monitored so that the Company is aware of its contractual rights and obligations in managing its Third Party relationships. Further attention shall be given to key dates and agreed upon items in the contract between the Company and the Third Party.

10. Oversight and On-Going Monitoring

10.1. **In General.** The Company shall maintain adequate oversight of Third Party activities and adequate quality control over those products and services provided through Third Party arrangements in order to minimize exposure to potential significant financial loss, reputation damage, product deterioration and legal/compliance risks. Third parties who fail to perform in a manner with the Company's performance standards and contractual requirements will be subject to demands for remedial action up to and including terminating the contract.

10.2. **Specific Oversight Standards.** As determined by the CCO**,** risk-based standards for oversight and monitoring may vary by business unit or functional area of the Company, and the nature and scope of the Third Party relationship. However, across all business units, the following applies:

Critical or High-Risk Third Party Relationships. Enhanced oversight procedures should be followed for any Third Party relationships (particularly those for Representatives) deemed critical or high-risk, including periodic reporting to and review by the Company's various committees or the Board, as appropriate.

Material changes. Procedures shall be adopted for managing changes in Third Party relationships, including changes identified in the Third Party risk review process, business-related changes to products or services, or other events that may reasonably necessitate contractual amendment, or otherwise warrant enhanced monitoring or oversight.

10.3. **Monitoring.** The extent and precise nature of oversight of a particular Third Party relationship will depend upon the identified risks of the Third Party relationship and/or recommendations from Senior

Management or the CCO. The Company shall maintain documents and records on all aspects of the Third Party relationship commensurate with the risk designation of the relationship. The BRO is responsible for monitoring the overall relationship with the Third Party and escalating any significant areas of concern to the head of the respective business unit, and or Senior Management, including deterioration in financial condition, service interruptions or other notable performance issues, security breaches or compliance issues or lapses.

10.4. **Reporting.** Ongoing reporting of oversight activity to appropriate committees of the Company and to the Board, as appropriate. Identified weaknesses should be documented and promptly addressed with business line management, with further escalation to Senior Management and the Board as appropriate.

11. Termination of Third Party Relationships

11.1. If, based on the monitoring that has been performed, or based on notification that has been received, it is determined that the Third Party no longer meets the requirements of the Company, other alternatives will be researched and the relationship with the Third Party may be terminated, if possible. Prior to termination, the responsible department will work with the CCO to develop contingency plans for outsourcing of the applicable product or service. Related considerations include:

- Capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.
- Risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the Third Party relationship.
- Handling of joint intellectual property developed during the course of the arrangement.
- Reputation risks to the Company if the termination happens as a result of the Third Party's inability to meet expectations.

11.2. At a minimum, the CCO will recommend that no other engagements be entered into with this Third Party until the identified deficiencies have been resolved and such recommendations will be reported to the Audit Committee. If it is determined that the Third Party is not meeting the intent of the agreement and has violated the performance measures and benchmark standards included in the contract, then the contract will be terminated in accordance with the provisions of the contract.

11.3. The Company will terminate Third Parties that commit crimes or violate applicable anti-corruption or anti-bribery laws. Any such terminations shall be documented pursuant to applicable record-keeping requirements.

12. Training

12.1. Appropriate Company Personnel will periodically attend training on managing Third Party relationships. The Company may require certain Company Personnel to receive training in the form of memos, in person presentations, webinars, or by articles/notices.

13. Compliance by Third Parties

13.1. Third Parties must abide by all applicable laws and regulations. The Company will provide copies of its Supplier Code of Conduct to Third Parties upon engagement, along with relevant policies

on an as-needed basis informed by procedures promulgated by the Company and will convey its expectation that those representatives will comply with the Code of Conduct and relevant policies.

14. Policy Administration & Review

14.1. Administration of this Policy is the responsibility of Chief Compliance Officer.

14.2. This Policy shall be reviewed at least once every three years or whenever a significant change occurs, including any change in law, that impacts the content or substance of this Policy.

*****

If you have questions about this Policy, please contact the Chief Compliance Officer.

*****