GROUP ETHICS & COMPLIANCE POLICIES

Speaking Up Policy | Conflicts of Interest Policy | Anti-Bribery & Corruption and Anti-Fraud Policy | Insider Trading Policy | Data Protection Policy | Business Partner Due Diligence Policy | Anti-Money Laundering Policy | Sanctions Policy | Antitrust Policy | Glossary | Last viewed page

Our Policies

Speaking Up Policy

Conflicts of Interest Policy

Anti-Bribery & Corruption and Anti-Fraud Policy

Insider Trading Policy

Data Protection Policy

Business Partner Due Diligence Policy

Anti-Money Laundering Policy

Sanctions and Trade Controls Policy

Antitrust Policy

SPEAKING UP POLICY

1. POLICY SUMMARY

- Summary
- Applicability
- What You Must Do
- Questions and Reporting Breaches

1. Policy Summary

1.1 Introduction

(a) We are committed to conducting our business in accordance with the highest ethical standards and to developing a culture built on trust and integrity where everyone feels comfortable to communicate any concerns, knowing that they will be addressed appropriately.

(b) This Policy sets out the procedures through which you can raise questions or concerns, or make reports about any suspected violations of:

(i) Applicable laws or regulations; and

(ii) Internal policies or guidelines, including the **Code of Ethics and Business Conduct**,

as well as how the **Ethics & Compliance Office** addresses reported concerns.

1.2 Applicability

This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible.

(c) Complete any training associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

2. POLICY REQUIREMENTS

- Raising Questions and Reporting Concerns
- How to Report a Concern
- Handling a Concern
- Investigating a Concern
- No Retaliation
- Your Responsibilities

2.1 Raising Questions and Reporting Concerns

(a) This Policy sets out the procedures through which you can raise questions or concerns, or make reports about any suspected violations of:

(i) Laws or regulations; and

(ii) Our internal policies or guidelines, including the **Code of Ethics and Business Conduct**.

Examples of what you must raise:

- Known or suspected **Bribery**, **Corruption**, or **Fraud**;
- Breaches related to **Trade Controls** or **Sanctions**;
- Actions or inactions that create a danger to the environment or the health and safety of any individual or group;
- Workplace harassment and discrimination; and
- Any actual or potential criminal offences or breaches of the **Code of Ethics & Business Conduct** or applicable laws or regulations.

(b) Any workplace interpersonal issues or Human Capital (HC) (also known as Human Resources or HR) grievances you may have (e.g., issues relating to remuneration or promotion) should be directed to either HC via the dedicated HC Grievance option within the confidential Helpline (located at **helpline.taqa.com**), or your **Manager** rather than through the processes set out in this Policy. The HC grievance process is managed by HC in accordance with their Policies and procedures.

2.2 How to Report a Concern

(a) To raise a concern, you may notify (depending on the nature of your concern):

(i) Your **Manager** or other internal management;

(ii) Your local HC representative;

(iii) Internal Audit; or

(iv) the **Ethics & Compliance Office** in person, or via the Ethics & Compliance/Non-HR Grievance option within the confidential Helpline (located at **helpline.taqa.com**). When using the Helpline, you may choose to be anonymous (where possible), but please be aware that if you do so, you should provide as much information as you can to allow for as thorough an assessment as possible.

(b) Concerns should only be raised in good faith where there is a genuine suspicion of wrongdoing. The Speaking Up process is there to help you raise concerns and should not be abused by raising intentionally false concerns. We have a zero-tolerance approach to retaliation against anyone who raises a concern, and those who engage in any retaliatory behavior will be subject to disciplinary action.

(c) You do not need to have absolute proof in relation to any concerns that you wish to raise. To enable us to investigate your concerns, you will need to be able to explain the reasons for your concerns, and it would be helpful if you provide sufficient details. For example, the individuals involved, witnesses, **Businesses**, dates, and any relevant times and events in chronological order.

(d) Your identity (or information that could lead to your identification) will only be shared on a 'need to know' basis and will be handled confidentially at all times.

(e) You may choose to remain anonymous when raising a concern, but please be aware that this could make any **Investigation** or assessment more difficult. Such anonymity will only be possible in accordance with applicable laws.

(f) Concerns should be raised promptly as this will improve the effectiveness of any subsequent **Investigation**.

(g) You must never attempt to conduct your own **Investigation** or interviews in relation to any concerns you may have as that may compromise the integrity of the **Investigation**. You must treat all information relating to any concern with utmost confidentiality and you must not, under any circumstances, discuss your concern with colleagues or **Third Parties** (unless otherwise required to by law).

2.3 Handling a Concern

(a) Any concerns will be assessed initially by the **Ethics & Compliance Office** to decide if an **Investigation** is needed and what form that **Investigation** should take.

(b) If the concern relates to the Group Chief Executive Officer and Managing Director of **TAQA Group**, the Board of Directors or the Chairman of the Board will be responsible for handling the concern and **Investigation**.

(c) If the concern relates to a member of the Board of Directors of **TAQA Group**, the Chairman of the Board will be responsible for handling the report and any **Investigation**. If the report relates to the Chairman of the Board, the other Board members will be responsible for handling the concern and any **Investigation**.

(d) If the concern relates to the Head of the **Ethics & Compliance Office**, the Chief Legal Officer will be responsible for handling the concern and any **Investigation**.

(e) If the concern relates to the Chief Legal Officer, the Group CEO will be responsible for handling the concern and any **Investigation**.

2.4 Investigating a Concern

(a) Where it is determined that an **Investigation** is required, an **Investigator** will be appointed. **Investigations** will take place whenever appropriate, irrespective of the seniority of the individuals involved or the issues at stake.

(b) Any information that you provide as part of an **Investigation**, or that is discovered during that **Investigation**, will be treated as confidential to the maximum extent possible. Information will only be disclosed on a 'need-to-know' basis.

(c) **Investigators** may seek assistance from other **TAQA Group Personnel** where necessary, provided those individuals do not have any relevant **Conflicts of Interest** and they are independent of the matter under **Investigation**.

(d) Where an **Investigator** is not a member of the **Ethics & Compliance Office**, their **Investigation** plan must be pre-approved by the **Ethics & Compliance Office**. The **Investigator** must liaise with the **Ethics & Compliance Office** throughout the course of the **Investigation** to provide updates and receive guidance.

(e) If appropriate, you will be informed of the closure of the **Investigation**, but (to protect the privacy of those involved) no feedback will be provided to you regarding the outcome of the **Investigation** or of any actions taken as a result of the **Investigation**.

2.5 No Retaliation

Concerns should only be raised in good faith. We have a zero-tolerance approach to retaliation against anyone who raises a concern or cooperates with an **Investigation**, and those who engage in any retaliatory behavior will be subject to disciplinary action.

2.6 Your Responsibilities

(a) You must cooperate when your assistance, or the assistance of someone you manage, is sought with respect to any **Investigation**. This means that you must:

(i) Make yourself, any persons that you manage, and any relevant documents and other records available to any **Investigator** or any other person who is assisting with an **Investigation**;

(ii) Be cooperative and truthful at all times;

(iii) Act in good faith and volunteer any information that may assist with an **Investigation**;

(iv) Maintain the confidentiality of any information that you receive as part of an **Investigation**, including the existence of the **Investigation**, the people involved, and the factual issues; and

(v) Not make recordings of any interviews conducted without the prior written consent of the **Ethics & Compliance Office**. An interview will only be recorded if the person being interviewed has been notified and given their consent to such recording.

CONFLICTS OF INTEREST POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

Policy Summary

1.1 Summary

(a) A **Conflict of Interest** arises when personal interests conflict with the interests of **TAQA Group**, or when judgement or decision-making is inappropriately influenced by external interests.

(b) **Conflicts** can be:

(i) Existing (actual **Conflict**);

(ii) A situation that could result in a **Conflict** (potential **Conflict**); or

(iii) A situation that could appear to be, but is in fact not, a **Conflict** (perceived **Conflict**).

(c) You have a duty to act in the best interests of **TAQA Group** and ensure that your personal interests do not interfere, or appear to interfere, with your ability to act in the best interests of **TAQA Group**.

(d) This Policy provides guidance on how to recognize a **Conflict of Interest** and how to disclose a **Conflict** to the **Ethics & Compliance Office**.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to all **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability and reputational damage. You may also be subject to disciplinary action, including termination of employment, and the possibility of civil and/or criminal penalties.

(c) **Businesses** may establish standards that are stricter than this Policy. Any exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible.

(c) Complete any training and required declarations associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

2. POLICY REQUIREMENTS

- Types of Conflicts
- Conflict of Interests Disclosure Process

Policy Requirements

We are committed to conducting our business with integrity and in accordance with the highest ethical standards. If a Conflict or the perception of one arises, you must disclose it to the Ethics & Compliance Office, this is to ensure that the potential Conflict is managed such that it does not affect your judgement and objectivity towards TAQA Group.

Conflicts arise in many different ways. A potential or perceived **Conflict** can be as harmful as an actual **Conflict**. A **Conflict of Interest** can arise based on your own interests or those of a **Related Person**.

If you find yourself in a situation where a **Conflict** could exist, you must disclose all of the facts of the situation to the **Ethics & Compliance Office**. Instructions on how to make a disclosure are included in section 2.3 of this Policy.

2.1 Types of Conflicts

The following sections set out some situations where a potential, actual, or perceived **Conflict** could exist. It is not possible to list every potential situation where a **Conflict** could arise, so it is important that you consider your actions carefully in the light of this Policy and raise any questions or concerns with the **Ethics & Compliance Office**.

(a) Personal Financial Interests

Having a **Financial Interest** in a **Third Party** that does business with **TAQA Group**, seeks or could potentially seek to do business with **TAQA Group** (excluding the provision of water and electricity services provided by **TAQA Group** to **Retail Customers**), or where the existence of that **Financial Interest** could otherwise interfere, or be perceived to interfere, with **TAQA Group**.

(b) Holding a Position as Officer or Director in a Third Party

(i) Having a position of **Officer** or **Director** in:

(A) a **Civic Organization**, even if you will not personally benefit from doing so;

(B) a **Government Entity**; or

(C) a **Third Party**, where the **Third Party** does business with **TAQA Group**, seeks or could potentially seek to do business with **TAQA Group**, or where the role may otherwise interfere, or be perceived to interfere, with your responsibilities to **TAQA Group**.

(ii) Serving on an Advisory Board for a **Third Party**.

(c) Other Relationships with Third Parties

(i) Being the local sponsor, or national agent, whether directly or indirectly, of any **Third Party** if they do business with or seek to do business with **TAQA Group** (may only apply in the UAE).

(ii) Providing services or support to a **Third Party** if it could affect the proper performance of your duty towards **TAQA Group**.

(iii) Accepting a personal loan or guarantee (other than those in respect of nominal monetary values) from a **Third Party** that seeks to do business with or does business with **TAQA Group**, except where that loan or guarantee is from a bank or other financial institution, and the loan or guarantee is on normal commercial terms.

(iv) Any **Lobbying** or **Political Contributions** must comply with the terms of the **Anti-Bribery & Corruption and Anti-Fraud Policy**.

(d) Employment

(i) Making decisions on, or being in a position to authorize or influence, the hiring, supervision, promotion or remuneration of a **Related Person** by **TAQA Group**.

(ii) Making decisions on, or being in a position to authorize or influence, any procurement decisions of a **Related Person** at **TAQA Group**.

(iii) Having a **Related Person** that is an employee of, or consultant to, or serves as an **Officer**, **Director**, or in another management position of a **Third Party** that seeks to do business with, does business with, or competes with **TAQA Group**.

(iv) Taking any external employment, including a part-time job, or provision of consulting services to an entity that seeks to do business with, does business with, or competes with **TAQA Group**. This includes the development and operation of a start-up.

(v) Using **TAQA Group** facilities, equipment, resources, personnel, materials, or working hours for any external employment or business activities, including a part-time job or the provision of consulting services.

(e) Related Persons

(i) Directing **TAQA Group** business to an entity that is owned, sponsored, or managed by a **Related Person**.

(ii) Using **TAQA Group** facilities, equipment, resources, personnel, materials, or working hours for the purposes of an entity that is owned, sponsored, or managed by a **Related Person**.

(iii) Engaging in a relationship that may conflict with your responsibilities to **TAQA Group** or compromise **TAQA Group** interests.

(f) Use of Confidential Information or TAQA Group Resources

You must carefully manage and protect **Confidential Information** belonging to or managed by **TAQA Group**, or for **Customers**, **Suppliers**, partners, and **TAQA Group Personnel**. Similarly, you must ensure that you are using any **TAQA Group** equipment, technology, and resources securely and appropriately. You must avoid any **Conflict of Interest** resulting from:

(i) Use of **TAQA Group Confidential Information**;

(ii) Use of **TAQA Group** facilities, equipment, IT resources, or working hours for part-time employment or other external consulting or business activities;

(iii) Misuse of **TAQA Group** resources, your position, or your influence in promoting or assisting a **Third Party**; and

(iv) Use of competitive **Confidential Information** for personal benefit.

In addition, it is against the law to trade **Securities** or tip off others to trade **Securities** based on **Confidential Information**. For more detailed guidance on trading **Securities**, refer to the **Insider Trading Policy**.

(g) Procurement

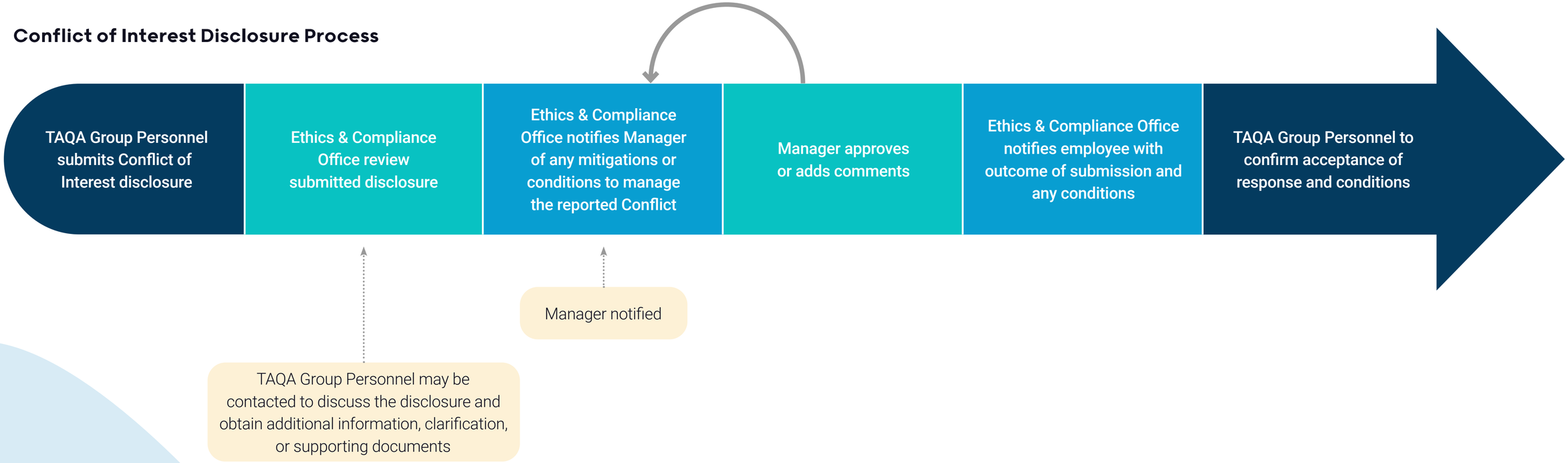
(i) Referring or participating in the review, selection, award, and/or administration of a contract where there may be a **Conflict of Interest** between you and a **Third Party**.

(ii) Approaching **TAQA Group Suppliers**, **Customers**, or other business relationships for donations to a charity or **Civic Organization** in which you are personally involved.

2.2 Conflict of Interests Disclosure Process

(a) **Conflicts** arise naturally at times. However, the existence of a Conflict does not necessarily mean that a breach of this Policy will occur. You must follow the process for disclosing a **Conflict of Interest** so we can assess whether it is possible to manage the **Conflict**, and to ensure we put the appropriate controls in place. If you have any doubts as to whether a **Conflict** exists, it is better to disclose your concerns so that the situation can be evaluated and appropriately addressed.

Conflict of Interest Disclosure Process



(b) In order for us to manage **Conflicts**, you must disclose any actual, potential, or perceived **Conflicts** by disclosing a **Conflict of Interest** through the Helpline (**helpline.taqa.com**). You must make this disclosure before engaging (or as soon as you become aware that you have engaged) in the activity to which the disclosure relates, and you must not proceed with the activity until you have received approval to do so from the **Ethics & Compliance Office**.

(c) When you disclose a potential **Conflict**, the **Ethics & Compliance Office** will review the disclosure and consult with your **Manager** to determine the appropriate course of action. The **Ethics & Compliance Office** will then inform you as to whether the situation is a **Conflict**, and, if so, whether or not it is manageable.

(d) If the **Ethics & Compliance Office** advises you that the **Conflict** is manageable, they will also explain to you how to manage the **Conflict**, including any specific actions that you must take.

(e) If the **Ethics & Compliance Office** advises you that the **Conflict** is not manageable, you must not engage in the activity which gives rise to the **Conflict**. Failure to disclose a **Conflict**, or delay in disclosure, may result in disciplinary action up to and including termination of employment.

(f) In addition, you will be asked periodically to certify that you understand this Policy and have disclosed all potential **Conflicts**.

(g) If you know or suspect that a member of **TAQA Group Personnel** has breached this Policy, you must report this to the **Ethics & Compliance Office** or anonymously submit a report through the channels described in the **Speaking Up Policy**.

3. FREQUENTLY ASKED QUESTIONS

Frequently Asked Questions

3.1 "When should I disclose a **Conflict of Interest**?"

*As soon as a potential or actual **Conflict** arises, you should disclose this through the Helpline at **(helpline.taqa.com)**.*

3.2 "I own a Facilities Management business and I wish to introduce it to the **TAQA Group**. I have disclosed a Conflict of Interest through the Helpline (**helpline.taqa.com**) relating to my business, can I now proceed with the introduction to **TAQA Group**?"

*You may only make the introduction when you have received an approval from the **Ethics & Compliance Office**.*

3.3 "A potential **Supplier** is a friend of my family. I would like to authorize the use of this **Supplier** for **TAQA Group** because I can get us a good deal. Can we use the **Supplier**?"

*You are allowed to introduce the **Supplier** to **TAQA Group**. However, you must fully disclose your relationship with the **Supplier** to the **Ethics & Compliance Office** who will assess whether it is appropriate to engage the **Supplier**.*

3.4 "My niece has just graduated from university and I think she is really well suited for a role within **TAQA Group**. Can **TAQA Group** hire her?"

*Your niece is a **Related Person** and must go through the normal formal recruitment process. You must disclose your relationship to the **Ethics & Compliance Office** who will ensure that you are not in any way involved in the recruitment process. The **Ethics & Compliance Office** will manage together with the business the decision relating to her employment, and you should not seek to influence the outcome in any way. If your niece is recruited, it should not be into a position where she reports directly or indirectly to you or where you have influence over her supervision, promotion, or remuneration.*

ANTI-BRIBERY & CORRUPTION AND ANTI-FRAUD POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

Policy Summary

1.1 Summary

(a) We are committed to conducting our business transparently and in accordance with the highest ethical standards. We have a zero-tolerance approach to all forms of **Bribery**, **Corruption**, and **Fraud**.

(b) As a global organization, we are subject to and comply with far reaching applicable laws and regulations designed to prevent **Bribery**, **Corruption**, and **Fraud**, and this Policy sets out guidance on how we prevent them.

(c) This Policy also sets out our position in relation to **Gifts**, **Hospitality**, and **Entertainment**, as well as speaking engagements and publications, **Sponsored Travel**, **Commercial Sponsorships**, **Charitable Donations** and **Grants**, requests by countries for payment, **Political Contributions** and **Lobbying**.

(d) This Policy is not intended to prevent legitimate activities directly related to the conduct of **TAQA Group's** business.

(e) If you have any doubts, questions or concerns about this Policy you should contact the **Ethics & Compliance Office** on the Helpline at (**helpline.taqa.com**).

(f) You must:

(i) Not offer, promise, or give a **Bribe** or other improper payment or advantage, directly or indirectly;

(ii) Not ask for or receive a **Bribe**;

(iii) Take extra care when dealing with **Public Officials**

(and you must avoid even the perception of any of the above);

(iv) Not make a **Facilitation Payment**, except where the making of such a payment is required to avoid risk to life or personal injury;

(v) Only engage in modest, reasonable, and appropriate expenditure on **Gifts**, **Hospitality**, and **Entertainment**. Pre-approval from your **Manager** and the **Ethics & Compliance Office** must be provided before the **Gift**, **Hospitality**, **Entertainment**, or **Sponsored Travel** is purchased, offered, or received, if the value threshold set out below in the Value Threshold Table is met or exceeded. This threshold applies whether such **Gifts**, **Hospitality**, **Entertainment**, or **Sponsored Travel** are offered or received on a one-off basis, or are cumulative over a six-month period to/from the same person or entity:

Value Threshold Table		
	Public Official	**Other**
Gifts, **Entertainment**, **Hospitality** and **Sponsored Travel** (per person present)	USD 0 AED 0	USD 150 AED 550

(vi) Obtain approval from the **Ethics & Compliance Office** (and in relation to points (i), (iii) and (iv) below, you will also need approval from Group Communications Department) before you:

(i) Agree to write any publications or participate in any speaking engagements for existing or potential **Suppliers**;

(ii) Accept any **Sponsored Travel**;

(iii) Agree to give any **Commercial Sponsorship**;

(iv) Provide any **Charitable Donations** or **Grants**;

(v) Agree to any requests for payments by countries or **Public Officials**; or

(vi) Give any **Political Contributions** or engage in any **Lobbying**;

(vii) Do not engage in any form of **Corruption** including **Fraud**; and

(viii) Conduct appropriate **Due Diligence** on **Business Partners** in accordance with the terms of the **Business Partner Due Diligence Policy** and be aware of any **Bribery** and **Corruption**-related risks.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability and reputational damage. You may also be subject to disciplinary action, including but not limited to termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** through the Contacts section available below, or through the channels described in the **Speaking Up Policy** (including the Helpline - **helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office**.

(c) Complete any training associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

2. POLICY REQUIREMENTS

- Bribery and Facilitation Payments
- General Requirements
- Gifts
- Entertainment and Hospitality
- Speaking Engagements and Publications
- Sponsored Travel
- Commercial Sponsorships
- Charitable Donations and Grants
- Requests by Countries for Payments
- Political Contributions & Lobbying
- Fraud
- Working with Business Partners

Policy Requirements

2.1 Bribery and Facilitation Payments

(a) **Bribery** and **Corruption** take many forms: they can be obvious, for example, a cash **Bribe**, or subtle, for example, job offers, commissions, or excessive **Hospitality**.

(b) **Facilitation Payments** are payments made to speed up or secure a routine government action.

(c) You must comply with the following requirements:

(i) Abide by all applicable laws and regulations;

(ii) Do not offer, promise, or give a **Bribe**, or other form of improper payment or advantage, directly or indirectly;

(iii) Do not ask for or accept a **Bribe**;

(iv) You must not indirectly **Bribe** by using intermediaries, such as agents, consultants, advisors, contractors, subcontractors, **Distributors**, any other **Business Partner**, or their **Family Members**;

(v) You must take extra care when dealing with **Public Officials** to avoid the perception of **Bribery** or **Corruption**;

(vi) Do not make **Facilitation Payments**, except where making such a payment is required to avoid risk to life or personal injury (in such circumstances, you must report the payment to the **Ethics & Compliance Office** as soon as you can and ensure that the payment is recorded properly in the relevant **Books and Records**);

(vii) In accordance with the terms of this Policy, you may engage in modest, reasonable, and appropriate expenditure for **Gifts**, **Hospitality**, **Entertainment**, and other legitimate activities directly related to the conduct of our business; and

(viii) You must immediately report to the **Ethics & Compliance Office** all instances where you think you may have offered, promised, or given a **Bribe** or where you may have asked for, or are offered, a **Bribe**.

Examples:

Bribing Another Person:
To secure a contract you offer a potential customer tickets to a major sporting event on the condition that they agree to switch suppliers away from a competitor and instead purchase our services.

*This would be a **Bribe** and a breach of this Policy.*

Bribing Another Person (Indirectly):
To help secure a contract, you hire a local agent to liaise with the potential customer. The agent requests funds from you and uses these funds to supply the customer with expensive gifts.

*This would be a **Bribe** and a breach of this Policy.*

Being Bribed:
In order to secure an engagement with us, a contractor offers you a free holiday on the condition that you agree to use the contractor's services on an upcoming energy project.

*This would be a **Bribe** and a breach of this Policy.*

Bribing a Public Official:
You arrange for the **Business** to make a payment to a customs official to speed up a customs clearance procedure. There is no formalized import fast-track system in place and no written law which would require such payment to be made.

*This would be a **Facilitation Payment** and a breach of this Policy.*

Protecting Life and Avoiding Personal Injury:
You are on business travel in a country where civil unrest breaks out and you have no alternative but to make a payment to a **Public Official** to get you on a flight out away from imminent danger.

*You would be able to make this payment, but you should report the payment to the **Ethics & Compliance Office** as soon as you can and ensure that the payment is recorded properly in the relevant **Books and Records**.*

2.2 Gifts, Hospitality, Entertainment, and Sponsored Travel - General Requirements

If the conditions and requirements set out in this Policy are met, we allow the offering and receiving of modest, reasonable, and appropriate **Gifts**, **Hospitality**, and **Entertainment** as they are an established part of doing business.

All **Gifts**, **Hospitality**, **Entertainment**, and **Sponsored Travel** must:

(a) Be for a legitimate business purpose, directly related to **TAQA Group** business, of a nature and value that is in line with industry norms in the place they are given or received, and modest, reasonable, and appropriate. The appropriate value will vary by country or region, and an acceptable value in some countries may be unacceptably high in others, so you must always be aware of the risk that even something of a low value may be inappropriate;

(b) Not be capable of being reasonably construed as a **Bribe**;

(c) Not put you or **TAQA Group** in a position that could compromise our reputation;

(d) Not be used to improperly influence, or appear to influence, you or anyone else, or have the intention of improperly obtaining or retaining business, or any other advantage;

(e) Not be offered to or accepted from a person or organization that has a reputation for dishonesty, or unethical or illegal conduct;

(f) Not be offered to or received from any party with whom we are engaged in an open bid or tendering process;

(g) Be pre-approved by your **Manager** and the **Ethics & Compliance Office** before the **Gift**, **Hospitality**, **Entertainment**, or **Sponsored Travel** is purchased, offered or received, if the value threshold set out below in the Value Threshold Table is met or exceeded. This threshold applies whether such **Gifts**, **Hospitality**, **Entertainment**, or **Sponsored Travel** are offered or received on a one-off basis, or are cumulative over a six-month period to/from the same person or entity (and note that it is your responsibility to monitor and record such **Gifts**, **Hospitality**, **Entertainment** and **Sponsored Travel** received cumulatively over time to ensure that you are aware if the threshold is met within a six month period). Pre-approval requests should be submitted through the Helpline (**helpline.taqa.com**).

Value Threshold Table		
	Public Official	**Other**
Gifts, **Hospitality**, **Entertainment** or **Sponsored Travel** (per person present)	USD 0 AED 0	USD 150 AED 550

If a pre-approval is not possible for legitimate reasons, then you must seek and obtain approval from your **Manager** and the **Ethics & Compliance Office** as soon as possible after purchasing, offering, or receiving the **Gift**, **Hospitality**, **Entertainment**, or **Sponsored Travel**. It is important that where **Gifts** are received without prior approval there is no perception that we have accepted a **Bribe**, so such **Gifts** must be handed over to the **Ethics & Compliance Office** who will arrange for them to be returned along with an appropriate explanation;

(h) Not breach any policies or local laws, rules, or regulations applicable to you or the person giving or receiving the **Gift**, **Hospitality**, **Entertainment**, or **Sponsored Travel**. It is your responsibility to check this;

(i) Not be offered to or discussed with **Public Officials**, or persons who might be perceived to be **Public Officials**, except with the pre-approval of the **Ethics & Compliance Office**. However, if as part of your role, or your team's role within **TAQA Group**, you have necessary regular meetings with **Public Officials** which may include the exchange of basic hospitality, such as coffee and light meals, you may request a blanket approval from the **Ethics & Compliance Office**. Such approval is to cover your interactions with that **Public Official** or **Government Entity** over a specific period, when you will not be required to submit multiple individual requests to approve **Gifts**, **Hospitality** and **Entertainment**. Reach out to the **Ethics & Compliance Office** to further understand the requirements surrounding this blanket approval process;

(j) Not be offered to you or another person indirectly, for example through a **Family Member**, or offered or given to any other person's **Family Member**;

(k) Not lead to an actual or perceived **Conflict of Interest**;

(l) Where required by this Policy, be approved by the **Ethics & Compliance Office**;

(m) Be supported by receipts (whenever possible) and be recorded fully and accurately in the relevant **Books and Records** of **TAQA Group** in a timely fashion and in line with applicable legal and accounting requirements; and

(n) Not conflict with any other policy obligations that you are subject to.

2.3 Gifts

In certain countries in which **TAQA Group** operates, **Gifts** are a reasonable and established part of doing business and can help to build better business relationships. The offering, giving, or receiving of **Gifts** is permitted provided that the requirements of this Policy are met:

(a) **Gifts** must never be cash or a cash equivalent such as a voucher or gift card. You must immediately notify the **Ethics & Compliance Office** of any cash or cash equivalent **Gifts** given, received, or requested;

(b) No **Gift** (of any kind or value, even customary) may be offered or provided by **TAQA Group Personnel** or **TAQA Group** to any Emirate of Abu Dhabi **Government Entity** and/or Abu Dhabi **Public Official** on a **Public Occasion**;

(c) **Gifts** should, wherever possible, be branded with a company logo to demonstrate their business purpose and limit their transferability;

(d) Any **Gifts** provided by **TAQA Group** to **TAQA Group Personnel** should be reasonable and proportionate given the recipient's tenure, level of seniority, and the circumstances in which the **Gift** is given. Where **Gifts** are given by **TAQA Group** to **TAQA Group Personnel**, they should be distributed in a fair and equitable way; and

(e) All **Gifts** exchanged between members of **TAQA Group Personnel** should be reasonable and appropriate in the circumstances, and should not be intended or perceived to influence the recipient's decision-making or objectivity in any way, particularly if the recipient is one of your **Managers** or superiors.

Gift or Bribe?

You are currently in contractual negotiations with a potential **Business Partner** in France. You receive tickets to an international football game in France from a senior **Director** of the **Business Partner**.

Gift *or* ***Bribe****? This could be a* ***Bribe*** *as the tickets have been provided during a period of ongoing negotiations and could be seen as an attempt to gain a business advantage. The tickets should be reported to the* ***Ethics & Compliance Office*** *who will advise of the appropriate action to take.*

Your team recently secured a significant deal with a **Business Partner** in North America. In celebration, your **Manager** takes the team and the **Business Partner** to lunch.

Gift *or* ***Bribe****? This is a* ***Gift****. It is not being given in an attempt to gain a business advantage as the deal has already been secured.*

You are given a branded plastic pen at a convention by a sales representative.

Gift *or* ***Bribe****? This is a* ***Gift****. Promotional gifts of low value such as branded stationery to or from existing or potential* ***Customers, Suppliers, and Business Partner*** *are acceptable.*

2.4 Entertainment and Hospitality

It is generally accepted business practice to offer or receive **Entertainment** and **Hospitality** that occur alongside business-related meetings and activities. Such **Hospitality** and **Entertainment** must be modest, appropriate, reasonable under the circumstances, and comply with the requirements of this Policy:

(a) At least one representative of **TAQA Group** and one representative from the recipient's organization must be present at the **Entertainment** or at an event where **Hospitality** is offered or received. Where multiple **TAQA Group Personnel** are involved in the offering and receiving of **Entertainment** or **Hospitality**, only one disclosure on behalf of the attending **TAQA Group Personnel** is required;

(b) When providing **Entertainment** or **Hospitality**, **TAQA Group** must, to the extent possible, pay for all costs directly, rather than the recipient paying such costs and then **TAQA Group** reimbursing them;

(c) When you are receiving **Entertainment** or **Hospitality**, the provider must, to the extent possible, pay for all costs directly, rather than you paying such costs and then the provider reimbursing you; and

(d) Any consumption of alcoholic beverages must be consistent with applicable internal policies (these may vary depending on the **Business**).

Examples:

- You catch a flight to the Netherlands to meet with a potential **Business Partner** to discuss a new project. The **Business Partner** books you into the presidential suite of the most expensive hotel in the city for the entire week when the meetings are only scheduled for three days.

  Entertainment/Hospitality *or a* ***Bribe****? This could be perceived to be a* ***Bribe****. The suite at the most expensive hotel goes beyond what would constitute reasonable business expenses and the length of the stay is excessive given the duration of the scheduled meetings. This should be immediately reported to the* ***Ethics & Compliance Office*** *who will advise you of the appropriate action to take.*

- You attend a client meeting and after the meeting has concluded, the client buys you lunch in the office canteen.

  Entertainment/Hospitality *or a* ***Bribe****? This is* ***Hospitality****. This would be common courtesy in most sectors and is unlikely to go beyond reasonable expenses. You would not need to disclose receiving this lunch if the value of the lunch is less than USD 150/AED 550 per person. Only in situations where the per person spend is expected to be higher than the USD 150/AED 550 per person threshold, or this* ***Hospitality*** *is offered by a* ***Public Official*** *(regardless of value), must a disclosure be submitted.*

2.5 Speaking Engagements and Publications

You may be invited to speak at events or conferences, give lectures, write publications, or participate in educational workshops. All of these opportunities may result in you receiving **Gifts**, **Hospitality**, and **Entertainment**, but even if they do not, such opportunities offer the recipient beneficial professional exposure which could be seen as a personal advantage, and therefore carry similar risks to those associated with the receiving of **Gifts**, **Hospitality**, and **Entertainment**.

To ensure compliance with this Policy, you must:

(a) Not write for any publications or participate in any speaking engagements for any **Third Party** with whom we are engaged in an open bid or tendering process;

(b) Disclose to the **Ethics & Compliance Office** if you receive any invitations from existing or potential **Business Partners** to speak at events or conferences, give lectures, write publications, or participate in educational workshops. Participation in such events is subject to the prior written approval of the **Ethics & Compliance Office** and must also be reported and approvals obtained (if required) in accordance with **TAQA Group's External Communications Policy**;

(c) Disclose to the **Ethics & Compliance Office** if you intend to invite any **Public Officials** to speak at events or conferences, give lectures, write publications, or participate in public educational workshops. Involvement in such events by a **Public Official** is subject to the prior written approval of the **Ethics & Compliance Office**; and

(d) Not accept any payment or fee in recognition of your contribution or work if the service you are asked to perform relates to your position or duties for **TAQA Group**.

Examples:

You are asked to speak as a member of a panel at an emissions reduction conference. The conference organizers offer to cover your travel and accommodation expenses.

*It should be disclosed to your **Manager** and to the **Ethics & Compliance Office** for approval if the conference organizer is a current or potential **Business Partner**. Additionally, Group Communications must also provide their approval in accordance with the **TAQA Group External Communications Policy**.*

2.6 Sponsored Travel

(a) Accepting **Sponsored Travel** may be appropriate if:

(i) The **Sponsored Travel** is for a legitimate business purpose;

(ii) The **Sponsored Travel** is no longer in duration than is necessary and only essential expenses are incurred. Any offers of per diem expenses should be disclosed to the **Ethics & Compliance Office** as we generally do not permit per diems to be paid to us by third parties unless set out in a legally binding agreement; and

(iii) Any costs are paid directly to service providers associated with the trip by the party providing the **Sponsored Travel**. This is to avoid the need for reimbursement to the party providing the **Sponsored Travel**. When this is not possible, it is best to use **TAQA Group** accounts to make payment for expenses rather than using personal accounts. All payments should be accounted for and invoices/ receipts should be issued/received (as appropriate).

(b) If the value of any **Sponsored Travel** meets or exceeds the value listed in the Value Threshold Table, then you must obtain prior written approval from the **Ethics & Compliance Office**. In cases where such pre-approval is not possible, you must then seek approval as soon as possible after the event.

Example:

A **Supplier** offers to pay for a flight to another country to attend a conference that they are hosting. They also have their company car drop you off to the hotel from the airport at their expense.

*If the total travel cost (flight and airport transfer) exceeds the value listed in the Value Threshold Table, you must obtain prior approval from the **Ethics & Compliance Office**.*

2.7 Commercial Sponsorships

Commercial Sponsorships can be used as a means of paying **Bribes**, so care must be taken before any arrangements are entered into and you must ensure that:

(a) All **Commercial Sponsorships** are formalized in a legally binding agreement. Your Legal department should help you with this agreement;

(b) Regardless of value, **Commercial Sponsorships** receive prior written approval by the **Ethics & Compliance Office**. You must also refer to the **TAQA Group Policy on Delegation of Authority** before entering into any **Commercial Sponsorship**; and

(c) You should refer to the **Global Sustainability Policy** (or any updated equivalent) for further guidance on **Charitable Donations** and the **TAQA Group Policy on Delegation of Authority** for further guidance before giving any **Grants**.

2.8 Charitable Donations and Grants

We sometimes provide **Grants** and make **Charitable Donations** for a variety of legitimate purposes.

To ensure that **Grants** and **Charitable Donations** cannot be seen to be **Bribes**, you must ensure that:

(a) **Grants** or **Charitable Donations** do not give rise to any immediate business advantage for **TAQA Group** and are not used to influence business;

(b) Regardless of value, **Grants** and **Charitable Donations** receive prior written approval from the **Ethics & Compliance Office**; and

(c) You refer to the **Global Sustainability Policy** for further guidance before offering or giving any **Grants** or **Charitable Donations**.

2.9 Requests by Countries for Payments

We operate in certain countries where it is permissible to make payments to governments at the government's request, for social or development purposes. Such payments are normally made as a condition for developing natural resources or to access certain associated governmental services. Any such payments must be legitimate, included within a legal agreement and/or permitted under local legislation, and the funds must be properly directed to the intended recipient(s).

In some countries, it is expected that **TAQA Group** will pay a daily allowance (or per diem) to cover the travel and daily living expenses of **Third Parties** associated with a project. Such per diems will only be payable by **TAQA Group** where properly documented in a legal agreement or where exceptional approval is provided by the **Ethics & Compliance Office**.

2.10 Political Contributions & Lobbying

Generally, we do not make **Political Contributions** or engage in **Lobbying** activity. All **Political Contributions** and **Lobbying** on behalf of **TAQA Group** should be disclosed to the **Ethics & Compliance Office** for approval.

Any personal political activities that you carry out should be kept separate from **TAQA Group** and you should never refer to **TAQA Group** or use **TAQA Group** resources for such personal political activities. You must ensure that your personal political activities are not linked to persons engaged in terrorism or criminal activities and do not cause any reputational damage for **TAQA Group**.

2.11 Fraud

Fraud can take many forms including falsifying accounts and making false expense claims. **Fraud** can be committed internally by **TAQA Group Personnel** and externally by our **Business Partners** and **Retail Customers**.

You must:

(a) Not engage in any **Fraud**;

(b) Protect our property and use it with care; and

(c) Understand the internal controls and procedures in the **Business** that you work for. Each **Business** must maintain policies and procedures designed to prevent **Fraud**.

Examples of Fraud:

- **TAQA Group Personnel** using their position for personal gain through the theft or misuse of **TAQA Group's** property or the property of anyone that **TAQA Group** has a relationship with;
- Destroying, defacing, concealing, or falsifying any **Books and Records**;
- Forging or altering any document including checks, bank documents, other financial documents, certified or legal documents, professional or educational qualification documentation, or forms of identification;
- Submitting false claims or invoices for payment or reimbursement;
- Making unauthorized disclosures or manipulating sensitive or **Confidential Information**; and
- Using deception for gain.

Red flags that may suggest that Fraud is taking place include:

- An unusually low or high turnover of key accounting and finance personnel in a **Business**;
- A **Business** being dominated by one individual where such individual is not effectively supervised or controlled;
- Lack of asset registers or inventory logs; or
- **TAQA Group Personnel** who have undisclosed **Conflicts of Interest** involving **Business Partners**.

2.12 Working with Business Partners

We engage the services of **Business Partners** to support our business activities and to participate in joint ventures and other business structures. These relationships are important to **TAQA Group** and provide valuable contributions in many areas of **TAQA Group's** business.

It is important that **TAQA Group** does not work with **Business Partners** that are involved in **Bribery**. It is therefore important to conduct the Due Diligence process set out in the **Business Partner Due Diligence Policy** and to ensure that your **Business Partners** attest to the **Business Partner Code of Conduct** by way of appropriate contractual provisions or otherwise. You must refer to the **Business Partner Due Diligence Policy** for further information and requirements in relation to **Business Partners**.

3. FREQUENTLY ASKED QUESTIONS

Frequently Asked Questions

3.1 "Can you please give me some examples of what might be a **Bribe**?"

*In addition to cash payments, a **Bribe** can include any offer, **Gift**, payment, promise to pay, or authorization for anything of value, such as:*

(a) ***Gifts**, **Hospitality**, and **Entertainment**;*

(b) Covering or reimbursing travel or accommodation expenses;

*(c) Offers of employment or other benefits to a **Family Member** or friend of another person;*

(d) Political party and candidate contributions;

(e) *Payments made through an agent or other **Third Party**;*

(f) Charitable contributions and sponsorships; and

(g) Investment opportunities, stock options or positions in joint ventures.

3.2 "The construction project I am working on is in desperate need of some specific materials but a local customs official will not release them, as he would ordinarily in the usual course of business, unless I give him a small cash payment – what should I do?"

*Making the payment to a local customs official in these circumstances would be considered a **Facilitation Payment** (a type of **Bribe**) and a breach of this Policy. You should refuse to make the payment and immediately inform the **Ethics & Compliance Office**. Please note that the same rules apply with respect to a payment made to the customs official via another party.*

3.3 "I am thinking about taking a **Business Partner** to an expensive restaurant and paying the bill. What should I do?"

*You should disclose this for pre-approval from the **Ethics & Compliance Office** if you expect the expenditure per person to be equal to or above the relevant value threshold as provided in the Value Threshold Table. (The per person expenditure would be calculated by dividing the total bill paid by the number of persons attending the meal).*

3.4 "We are pursuing business from a **Government Entity**, and common practice in this region involves retaining local "agents" who facilitate winning such business. Is this appropriate?"

*You must not pay **Bribes** to **Government Entities**, **Public Officials**, or any other persons directly or indirectly; this includes **Bribes** made via an "agent" or other **Third Party**.*

3.5 "I have received a **Gift** from a bidder during a tender process – what should I do?"

*You should immediately disclose and pass the **Gift** onto the **Ethics & Compliance Office** along with details of who gave it to you. The **Ethics & Compliance Office** will arrange the return of the **Gift** and contact the person who gave it to you to explain why it is being returned.*

3.6 "My local football team has approached me to ask for sponsorship. Can **TAQA Group** sponsor the football team?"

Yes, provided that the following conditions are met:

*(i) The sponsorship is in line with **TAQA Group's** sponsorship strategy;*

(ii) The sponsorship is formalized in a legally binding agreement; and

*(iii) Prior written approval is obtained from the **Ethics & Compliance Office**.*

3.7 "I have noticed that my colleague appears to put in a lot of travel expense claims, when I am not sure they ever go out of the office for work – should I be worried?"

*Making false expense claims is **Fraud** and a breach of this Policy and will be against the law in most cases. You must report your concerns to the **Ethics & Compliance Office**, through the channels described in the **Speaking Up Policy** as soon as possible and they will provide you with advice.*

4. PRE-APPROVALS PROCESS

Pre-Approvals Process

Where pre-approval from the **Ethics & Compliance Office** is required by this Policy you must:

(a) Seek approval from your **Manager** before requesting approval from the **Ethics & Compliance Office** (in respect of **TAQA Group Personnel** based in the UAE through the Helpline (**helpline.taqa.com**); and

(b) For all approvals whether for **Gifts**, **Hospitality** and **Entertainment**, or for anything else (such as speaking engagements and publications, **Sponsored Travel**, **Commercial Sponsorships**, **Grants**, requests by countries for payments, and **Political Contributions** and **Lobbying**), you must submit a request for approval through the Helpline (**helpline.taqa.com**).

INSIDER TRADING POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

Policy Summary

1.1 Summary

(a) This Policy provides guidance to assist you in understanding your responsibilities regarding **Trading** in **Securities**, including:

- (i) Your obligations to protect **Material Confidential Information**;
- (ii) When you may **Trade** in **TAQA Group Securities**; and
- (iii) Disclosure requirements related to your personal **Trading** in **TAQA Group Securities** and that of your **Related Persons**.

(b) You may **Trade** in **TAQA Group Securities** in a personal capacity provided that you:

- (i) Obtain prior written approval from the **Ethics & Compliance Office**;
- (ii) Obtain prior written approval from the relevant exchange (where required); and
- (iii) Comply with all requirements as provided in this Policy.

(c) In the event that you, or your **Related Persons** (to the best of your knowledge), hold any **TAQA Group Securities**, you must disclose such holdings to the **Ethics & Compliance Office**. You must also disclose any **Trading** in **TAQA Group Securities** by you, or (to the best of your knowledge) your **Related Persons**. You are also obliged to notify **ADX** of any such **Trade** by you or your **Related Persons** on the **ADX** and you must inform your **Related Persons** of their obligation to obtain approval from **ADX** prior to such **Trade**.

(d) If you are a **Restricted Person** there are additional disclosure obligations relating to you and your **Related Persons** when **Trading** in **TAQA Group Securities** listed on the **LSE** (as further detailed in Section 2.5).

(e) It is illegal to **Trade**, in any **Security** directly, or indirectly (i.e., either by yourself, by a **Related Person**, or someone acting on your behalf e.g. an investment manager), or to encourage others for the benefit of yourself or others to **Trade**, when in possession of **Material Confidential Information**, as this is considered **Insider Trading**.

(f) You are not permitted to **Trade** in **TAQA Group Securities** during any **Closed Periods** or **Blackout Periods** (even if you have already obtained approval to **Trade**).

(g) This Policy is to be read in conjunction with the **Code of Ethics & Business Conduct** and any other relevant policies and procedures.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability, and reputational damage. You may also be subject to disciplinary action, up to and including termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** through the Contacts section available below or through the channels described in the **Speaking Up Policy**.

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics and Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office**.

(c) Complete any training and required declarations associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations, you must comply with such laws or regulations rather than with this Policy.

2. POLICY REQUIREMENTS

Prohibition on Insider Trading and Encouraging Others to Trade

Personal Trading

Approvals Process

Disclosure Requirements for Related Persons

Additional Requirements for Restricted Persons

Closed Periods & Blackout Periods

Other External Requirements and Considerations

Protection of Material Confidential Information

Exceptions to the Policy

Policy Requirements

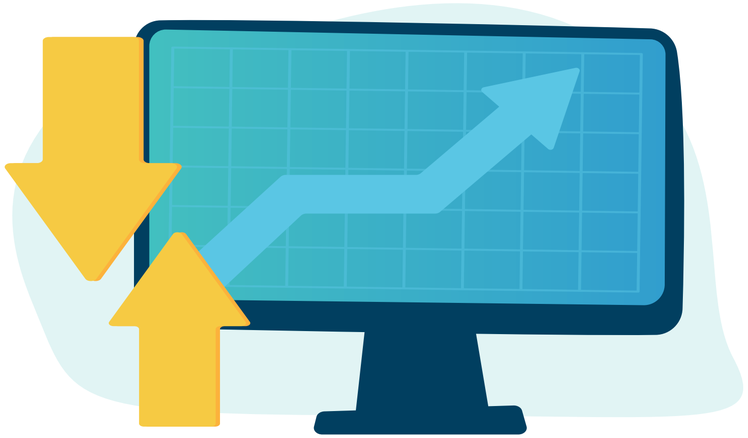
2.1 Prohibition on Insider Trading and Encouraging Others to Trade

(a) It is illegal to **Trade** in **Securities** (including **TAQA Group Securities**), either directly or indirectly, for the benefit of yourself or others, when you are in possession of **Material Confidential Information** about those **Securities** (making you an **Insider**) as this is considered to be **Insider Trading**. It is also illegal to recommend or encourage others to **Trade** in **Securities** (including **TAQA Group Securities**) for the benefit of yourself or others, whilst in possession of **Material Confidential Information**, even if you will not profit from such **Trading**.

(b) Whether you are in possession of **Material Confidential Information** will depend on the facts of the particular situation. Examples of information that would usually be considered material include, but are not limited to, the following types of information when not publicly available:

- (i) Earnings guidance and financial results;
- (ii) Potential or actual gain or loss of a significant **Customer** or **Supplier**;
- (iii) Pending or proposed mergers, acquisitions, restructurings, joint ventures, tender offers, or changes in assets;
- (iv) Entry into or cancellation of significant contracts or financial obligations;
- (v) Plans to go into a new line of business or launch a new product;
- (vi) Changes in pricing policies;
- (vii) Borrowing activities (other than in the ordinary course of business);
- (viii) A capital raising or other funding initiative;
- (ix) Changes in dividend policy or capital structure (such as a stock split, changes to rights of security holders, defaults, additional security sales, etc.);
- (x) Pending or threatened material litigation or regulatory action;
- (xi) Change of external auditors;
- (xii) Board or senior management changes;
- (xiii) Liquidity or anticipated credit rating changes;
- (xiv) Impending bankruptcy, receivership, or material cash flow changes;
- (xv) Knowledge of a prospective significant **Trading** in a **Security**;
- (xvi) Changes in information previously disclosed to the market; and
- (xvii) Any other information as included in a definition of **Material Confidential Information** (or equivalent defined term) in the relevant regulations issued by any applicable exchange on which **TAQA Group Securities** are listed.

(c) Determining what is **Material Confidential Information** is often difficult, particularly when information comes from, or directly relates to, a **Third Party**. If you are not sure whether information you have come across is **Material Confidential Information** and you want to **Trade** in **Securities** to which such information is related, or if you believe you may have **Traded** while in possession of **Material Confidential Information**, you must immediately contact the **Ethics & Compliance Office**.



2.2 Personal Trading

(a) You may **Trade** in **Securities** (including **TAQA Group Securities**) in your personal capacity as long as you do not breach this Policy or any applicable law or regulation.

(b) You must disclose any holdings in **TAQA Group Securities** to the **Ethics & Compliance Office** through the Helpline (**helpline.taqa.com**).

(c) If you are in possession of **Material Confidential Information** relating to **TAQA Group** you must not **Trade** in **TAQA Group Securities** or request approval to **Trade** through the Helpline (**helpline.taqa.com**). If you become aware that you are, or may be in possession of **Material Confidential Information** relating to **TAQA Group** after you request approval to **Trade**, you must inform the **Ethics & Compliance Office** as soon as possible and you must refrain from **Trading** in any **TAQA Group Securities** (even if you have already been given approval to **Trade**).

2.3 Approvals Process

(a) You may **Trade** in **TAQA Group Securities** in a personal capacity (including any **Third Party** trading on your behalf), provided that you have notified and obtained prior approval from the **Ethics & Compliance Office** (such approval to be at the sole discretion of the **Ethics & Compliance Office**), you have obtained clearance to **Trade** from **ADX**, and such **Trading** does not take place in a **Closed Period** or a **Blackout Period**.

(b) Applications for clearance to **Trade** should be made through the Helpline (**helpline.taqa.com**). If you have received approval from the **Ethics & Compliance Office** (which may be given with conditions which must be followed), you have 2 **Business Days** to apply for approval to **Trade** from **ADX** using the **ADX** Clearance to Trade Form available to be downloaded through the Helpline (**helpline.taqa.com**) (or the latest version as required by **ADX**). For **TAQA Group Securities** listed on markets other than **ADX**, it is your responsibility to obtain the necessary approvals (if any) from the relevant market.

(c) Once you have submitted the **ADX** Clearance to Trade Form you must notify the **Ethics & Compliance Office** through the Helpline (**helpline.taqa.com**), confirming that you are seeking **ADX** clearance to **Trade**, or whether you have chosen not to proceed with the **Trade**.

(d) Upon receiving approval to **Trade** from **ADX**, you must notify **Ethics & Compliance Office** through the Helpline (**helpline.taqa.com**).

(e) Should you wish to proceed with the **Trade**, you must do so within 2 **Trading Days** from receiving the **ADX** approval (or within 2 **Trading Days** of receiving approval from the **Ethics & Compliance Office**, where additional approvals from the relevant market are not required). You must then notify the **Ethics & Compliance Office** whether or not such **Trade** has been completed or not within 1 **Business Day** following expiry of the relevant 2 **Trading Day** period, through the Helpline (**helpline.taqa.com**).

(f) If a 2 **Trading Day** window overlaps with a **Closed Period** or **Blackout Period**, then any approval obtained from either the **Ethics & Compliance Office** or **ADX** will be null and void, and you must request approval again through the Helpline (**helpline.taqa.com**), if you still wish to **Trade**.

If you fail to meet the prescribed timelines relating to approvals and notifications set out in this Section 2.3, yet still wish to **Trade**, then you must start the approval process again through the Helpline (**helpline.taqa.com**).

(g) If you execute the **Trade** mentioned in (e) above you will not be permitted to make any further **Trades** in any **TAQA Group Securities** for a period of 60 days following the initial **Trade**. The **Ethics & Compliance Office** may consider exceptions to this restriction, but any exceptions will be considered on a case by case basis by the **Ethics & Compliance Office** in the event that you request approval to **Trade**.

2.4 Disclosure Requirements for Related Persons

(a) You must disclose any holdings in **TAQA Group Securities** by your **Related Persons** as and when it comes to your knowledge, through the helpline (**helpline.taqa.com**).

(b) If you become aware that a **Related Person** intends to **Trade** or has **Traded** in any **TAQA Group Securities** listed on **ADX**, you must notify the **Ethics & Compliance Office** through the helpline (**helpline.taqa.com**) within 5 **Business Days** of this information coming to your attention. You are also obliged to notify **ADX** of the **Trade** using the **ADX** Clearance to Trade Form available to be downloaded through the Helpline (**helpline.taqa.com**) (or the latest version as required by **ADX**), and you must inform your **Related Persons** of their obligation to obtain approval from **ADX** prior to such **Trade**.

2.5 Additional Requirements for Restricted Persons

(a) The **Ethics & Compliance Office** will notify you if you are a **Restricted Person**.

(b) There are additional specific requirements that apply to you as a **Restricted Person**, if you, your **Related Persons** or your investment manager seek to **Trade** in **TAQA Group Securities** listed on the **LSE**. These requirements are as follows:

- As a **Restricted Person** you are required to disclose any **Trades** regardless of value, in **TAQA Group Securities** by you, your **Related Persons** or your investment manager to the **FCA** within 2 **Business Days** of the relevant **Trade**.
- **Restricted Persons** are also required to notify their **Related Persons** and any investment manager of these disclosure requirements and to request that they do not **Trade** in any **TAQA Group Securities** during a **Closed Period** or a **Blackout Period**.

2.6 Closed Periods & Blackout Periods

(a) You must not **Trade** in any **TAQA Group Securities** during a **Closed Period** or a **Blackout Period**, whether directly or indirectly, even if you have been granted approval.

(b) **Related Person**

You must also disclose any **Trading** in **TAQA Group Securities** by a **Related Person** that you are aware of during any **Closed Period** or **Blackout Period** or during a period in which you are in possession of **Material Confidential Information** to the **Ethics & Compliance Office**. Such disclosure should be made prior to the **Trade** where possible, or as soon as you become aware of such **Trade** taking place.

(c) **Investment Managers**

You must advise all investment managers acting on your behalf:

(i) Of the **Closed Periods** and **Blackout Periods** during which you are not permitted to **Trade** (directly or indirectly) in **TAQA Group Securities**; and

(ii) That they must advise you immediately after they have **Traded** in **TAQA Group Securities**. In the event that a **Trade** has taken place during a **Closed Period** or **Blackout Period**, then you are obliged to notify the **Ethics & Compliance Office**.

The table below summarizes the requirements for **Trading** in **TAQA Group Securities** covered in Sections 2.2 to 2.6 above. The sequence which should be followed regarding the approvals and notifications related to **Trading** is indicated by the numbers in the colored circles below.

		Disclosures	Approvals	Notifications	Restrictions/ limitations
Requirements for all TAQA Group Personnel	**TAQA Group Personnel and Investment Managers acting on their behalf**	Holdings and Trades in TAQA Group Securities to the E&C Office.	1 Seek Prior approval from E&C Office for Trading in TAQA Group Securities. If approved 2 Seek approval from ADX within 2 Business Days of E&C approval.	3 Notify E&C Office whether or not ADX Clearance Trade to Form has been submitted. 4 Notify E&C Office if ADX clearance has been obtained (2 Trading Days Trading window). 5 Notify E&C Office whether or not approved Trades have taken place within 1 Business Day following the 2 Trading Days Trading window. 6 Notify E&C Office at any point if you come into possession of Material Confidential Information following any request for approval to Trade, and Trading should ceased.	Refrain from Trading in TAQA Group Securities when in possession of Material Confidential Information. No Trades in any TAQA Group Securities during a Closed Period or a Blackout Period. Trading in TAQA Group Securities is not permitted for a period of 60 days following any Trade in TAQA Group Securities.
	Obligations on all TAQA Group Personnel in respect of Related Persons	Holdings and Trades in TAQA Group Securities (to the best of knowledge) to E&C Office. Trades in TAQA Group Securities during any Closed Period or Blackout Period or whilst in possession of Material Confidential Information to E&C Office.		Notify E&C Office when Related Persons intend to Trade or have Traded in any TAQA Group Securities listed on ADX within 5 Business Days. Notify ADX of the Related Person's Trade using the ADX Clearance to Trade Form. Notify Related Persons of their obligation to obtain approval from ADX prior to such Trade.	
Additional Requirements for Restricted Persons	**Individual Restricted Persons and Investment Managers acting on their behalf**	Trades in LSE listed TAQA Group Securities to the FCA within 2 Business Days of the relevant Trade		Must notify Related Persons and Investment Managers of disclosure requirements, and not to Trade in TAQA Group Securities during a Closed Period or Blackout Period.	
	Obligations on Restricted Persons in respect of their Related Persons				

1 5 *Applicable to **Trading** of **TAQA Group Securities** on any exchange.*

2 3 4 *Only applicable for **Trading** of **TAQA Group Securities** listed on the **ADX**.*

6 *Only applicable if you come into possession of **Material Confidential Information**.*

2.7 Other External Requirements and Considerations

(a) You must not engage in **Market Manipulation** in respect of **TAQA Group Securities**. This means that you must not **Trade**, distribute information, or otherwise behave in a way that is likely to affect an investor's decision to invest in **TAQA Group Securities** by giving that investor a false or misleading impression about the supply, demand, price, or value of **TAQA Group Securities**.

(b) **Trading** in **Securities** may trigger additional disclosure or pre-approval requirements that are beyond what is required by **TAQA Group**. It is your responsibility to find out what legal and regulatory requirements apply to your **Securities** transactions and ensure that you comply with such requirements.

(c) You may, from time to time, receive **Material Confidential Information** about a listed company in the course of your duties at **TAQA Group**. You must not, directly or indirectly **Trade** in, or encourage others to **Trade** for the benefit of yourself or others, in **Securities** related to that listed entity while in possession of **Material Confidential Information**.

(d) If you leave **TAQA Group**, you will remain subject to this Policy until the later of:

(i) Such time as **TAQA**, or any other entity within the **TAQA Group** announces its next quarterly financial results; or

(ii) You are no longer in possession of **Material Confidential Information** relating to **Securities**.

2.8 Protection of Material Confidential Information

(a) **Material Confidential Information** relating to **TAQA Group** should only be disclosed to recipients who are authorized to receive such information, or to third party advisors who are contractually required to keep the information confidential. If you need to share **Material Confidential Information** with anyone who is not authorized to receive such information, you must obtain prior approval from the **Ethics & Compliance Office**.

(b) When disclosing, sharing, or exchanging **Material Confidential Information** in the course of your role at **TAQA Group**, you must ensure that the recipient understands that the information is confidential, and has provided a commitment to keep such information confidential through a written agreement drafted or reviewed by your Legal Counsel prior to receiving any **Material Confidential Information**.

(c) If you receive requests to speak about or share **Material Confidential Information** with the media or any other third party, you must not respond to those requests, and you must immediately contact the **Ethics & Compliance Office** and Group Communications Department.

(d) If you are not sure whether information is **Material Confidential Information** and is therefore subject to disclosure restrictions, or if you believe you may have disclosed **Material Confidential Information** in breach of this Policy, immediately contact the **Ethics & Compliance Office**.

2.9 Exceptions to the Policy

The requirements of this Policy do not apply when **Trading** in **TAQA Group Securities** via the following investment vehicles:

- Exchange Traded Funds (ETFs), mutual funds, unit investment trusts, and similar entities.
- Personal accounts over which an employee has no direct or indirect influence or control (e.g., a Discretionary (or Managed) Account, blind trust etc.)
- Pension funds, US - 529 accounts, 401k retirement accounts, or similar in other jurisdictions.

3. FREQUENTLY ASKED QUESTIONS

Frequently Asked Questions

3.1 "Who is an **Insider**?"

*Any individual who is in possession of **Material Confidential Information** relating to **Securities** (including **TAQA Group Securities**) is an insider. External advisors and other third parties may also be **Insiders**.*

3.2 "I recently joined **TAQA Group** and I own **TAQA Group Securities** in my personal portfolio. What are the requirements if I was to **Trade** in **TAQA Group Securities**?"

*Firstly, you should disclose your ownership in **TAQA Group Securities** to the **Ethics & Compliance Office** following the process mentioned in Section 2.2 (b) above. Secondly, you should obtain approvals from the **Ethics & Compliance Office** and **ADX** (where applicable) following the approvals and notification process set out in Section 2.3 above.*

3.3 "I have learned that **TAQA Group** is considering the acquisition of a small, publicly traded company. My brother just lost his job and really needs money to support his family. Since it will not benefit me personally, can I tell him about this so he can acquire **Securities** in the **Business** in anticipation of the acquisition?"

*No. **Trading** when in possession of **Material Confidential Information** is illegal and a violation of this Policy, whether **Trading** in **TAQA Group Securities** or the **Securities** of another company. The rules do not only prohibit you from buying or selling **Securities** but also from encouraging others to do so. Do not share the information with your brother or anyone else. If you have additional questions, you should contact the **Ethics & Compliance Office** for guidance.*

3.4 "Due to the nature of my job, I have become aware of information that I believe is **Material Confidential Information**, but is not being treated as confidential. What should I do?"

*You must not discuss or share the information with anyone and should immediately inform the **Ethics & Compliance Office**.*

DATA PROTECTION POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

What Information is Subject to this Policy?

1. Policy Summary

1.1 Summary

(a) **TAQA Group** collects, stores and **Process Personal Data** as part of its operations. This may include the **Personal Data** of its current, past and prospective employees, contractors, and the business contacts of its suppliers and customers. Protecting the confidentiality and integrity of such **Personal Data** is a responsibility that **TAQA Group** takes seriously.

(b) **TAQA Group** is a global organization operating in different sectors and markets and is subject to various laws and regulations relating to the **Processing** of **Personal Data**. This Policy, together with any other policies implemented by the **Business**, sets out the requirements and standards that **TAQA Group Personnel** must adhere to, including to ensure that **TAQA Group** complies with all applicable **Data Protection Laws**.

(c) To ensure **TAQA Group** complies with applicable **Data Protection Laws**, all **TAQA Group Personnel** are required to comply with the nine (9) principles detailed in section 2- ("**Data Processing Principles**") as summarized below.

In summary, these nine (9) principles require that:

1. We **Process Personal Data** lawfully, fairly and in a transparent manner (section 2.1 Lawfulness, Fairness, Transparency);
2. We collect **Personal Data** only for specified, explicit and legitimate purposes and it is not **Processed** in a manner that is incompatible with those purposes (section 2.2 Purpose Limitation);
3. **Personal Data** is adequate, relevant and limited to what is necessary in relation to the purposes for which it is **Processed** (section 2.3 Data Minimization);
4. **Personal Data** is accurate and, where necessary, kept up to date (section 2.4 Accuracy);
5. We keep **Personal Data** for no longer than is necessary for the purposes for which the **Personal Data** is **Processed** (section 2.5 Storage Limitation);
6. We **Process Personal Data** in a manner that ensures appropriate security of **Personal Data** (section 2.6 Integrity and Confidentiality);
7. We are able to demonstrate compliance with these principles (section 2.7 Accountability);
8. We **Process Personal Data** in accordance with the rights of **Data Subjects** (section 2.8 **Data Subject Rights**); and
9. Any transfers of **Personal Data** only occur where appropriate protections are in place and in compliance with applicable **Data Protection Laws** (section 2.9 Sharing Personal Data).

The first seven (7) of these principles (also mentioned in sections 2.1 to 2.7) reflect the General Data Protection Regulation's (**GDPR**) key data processing principles (which is the internationally recognized standard for data protection). The final two (2) principles (sections 2.8 and 2.9) reflect other core requirements under applicable **Data Protection Laws** with which **TAQA Group** will comply.

(d) Further requirements of **TAQA Group** and **TAQA Group Personnel** in relation to matters such as keeping written records and reporting **Personal Data** breaches are set out in this Policy (section 3 Additional Policy Requirements).

(e) Each **Business** is required to maintain internal processes and procedures that give effect to this Policy.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and **TAQA Group Personnel**.

(b) Failure to follow this Policy puts you, your colleagues and **TAQA Group** at risk of civil and/or criminal liability and reputational damage. You may also be subject to disciplinary action, including but not limited to, termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

(d) There is a grace period of one year from the launch of this Policy for the respective business leaders to ensure that there are sufficient procedures and processes in place, in order to fully implement this Policy.

1.3 What You Must Do

- Understand and comply with the requirements of this Policy, the **Code of Ethics and Business Conduct** and any standards introduced by the **Business** in which you work.
- Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office**.
- Complete any training associated with this Policy.
- Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

1.5 What Information is Subject to this Policy?

(a) This Policy applies to our management of **Personal Data**, which includes any information that may identify a **Data Subject**. This can include:

(i) Any information that may identify a **Data Subject** directly (such as a name, email address, or identification/reference number); or

(ii) Any information that may identify a **Data Subject** indirectly, either alone or in combination with other identifiers (such as a phone number, address, online identifier, or online location data).

(b) This Policy also applies to the **Processing** of **Special Category Data**. This includes "sensitive" **Personal Data** revealing (among other things) a **Data Subject**'s racial or ethnic origin, political opinions, religious or philosophical beliefs, and health. Some of the **Data Protection Laws** applicable to **TAQA Group** impose more stringent requirements in relation to the **Processing** of **Special Category Data**. **TAQA Group** implements controls that are appropriate to the sensitivity of the **Personal Data** that it **Processes**.

2. DATA PROCESSING PRINCIPLES

- Lawfulness, Fairness, Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability
- Data Subject Rights
- Sharing Personal Data

2. Data Processing Principles

2.1 Lawfulness, Fairness, Transparency

(a) We will **Process Personal Data** lawfully, fairly, and in a transparent manner. This means that we can only **Process Personal Data** where we have a lawful basis to do so. We can **Process Personal Data** on the basis of any of the following:

(i) Where the **Data Subject** has given their consent. To satisfy **GDPR,** it is important to note that for any consent to be valid, it must be given freely and the **Data Subject** must have been properly informed as to the **Processing** of their **Personal Data**;

(ii) Where the **Processing** is necessary for the performance of a contract with the **Data Subject**;

(iii) Where it is necessary to meet **TAQA Group's** legal compliance obligations;

(iv) Where it is necessary to protect the **Data Subject's** vital interests;

(v) Where the **Processing** is carried out in the public interest; or

(vi) Where the **Processing** is necessary for the purposes of our legitimate business interests (except where such legitimate interests are overridden by the interests of the applicable **Data Subject**).

(b) Where we **Process Personal Data** based on our legitimate business interests, such interests should be set out in any applicable privacy notice. We must also document why it was concluded that relying on **TAQA Group's** legitimate business interests was an appropriate legal basis to **Process** the **Personal Data**.

(c) We are also required, pursuant to the **GDPR**, to provide certain minimum information to **Data Subjects**, about our data processing activities, using clear and plain language.

2.2 Purpose Limitation

(a) We only collect **Personal Data** for specified, explicit and legitimate purposes and we do not **Process** any such data in a manner that is incompatible with these purposes. A new purpose may be 'incompatible' with the original purpose, depending on factors including:

(i) Any link between the original purpose and the new purpose;

(ii) The context in which the **Personal Data** was originally collected – in particular, our relationship with the **Data Subject** and what that **Personal Data** would reasonably expect;

(iii) The nature of the **Personal Data**, in particular its sensitivity;

(iv) The possible consequences for **Data Subjects** of the new **Processing**; and

(v) Whether there are appropriate safeguards in place, such as the replacement or removal of information that identifies an individual via relevant security/technical controls/measures.

(b) Where we wish to use **Personal Data** for a purpose that is incompatible with the original purpose for which it was collected, we must first obtain the relevant **Data Subject's** consent to **Process** the **Personal Data** for that new purpose.

2.3 Data Minimization

We will only **Process Personal Data** that is adequate, relevant and limited to what is necessary in relation to the purposes for which such **Personal Data** is **Processed**. This means that we will only collect the minimum amount of **Personal Data** that we require to achieve the purpose for which we have collected that data.

2.4 Accuracy

(a) We will ensure that all **Personal Data** that we **Process** is accurate and, where necessary, kept up-to-date and it is the responsibility of each individual **Business Leader** to appoint a **Data Protection Controller** within its business. Where we discover that any **Personal Data** that we have collected is misleading or incorrect, we will take reasonable steps to correct or erase the data as soon as possible.

(b) Our obligation to ensure that the **Personal Data** that we **Process** is up-to-date will depend on the circumstances, and should take into account potential consequences for the relevant **Data Subject** if such **Personal Data** is not kept up-to-date (e.g. where a mistake may result in an intended payment due to a **Data Subject** being sent to an incorrect bank account).

2.5 Storage Limitation

We store and retain **Personal Data** for no longer than is necessary for the purposes for which the **Personal Data** is **Processed**. This period will depend on the stated purposes for which we **Process** such **Personal Data**, or whether there are any applicable legal or regulatory requirements that may require us to retain such **Personal Data**.

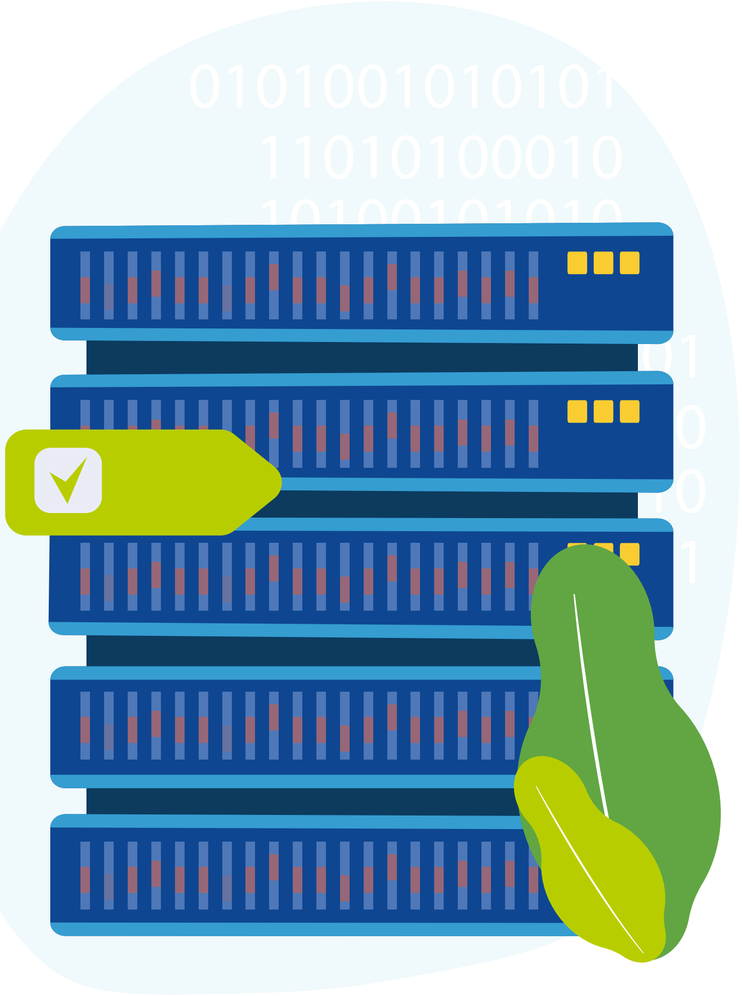
2.6 Integrity and Confidentiality

We implement appropriate organizational and technical measures to protect against any unauthorized or unlawful **Processing** and against accidental loss, destruction or damage of **Personal Data**. This includes technical IT security measures (such as password protections and authorized access requirements) and document management protocols (such as secure locking of physical documents and paper shredding requirements). These safeguards are proportionate to our size, scope and business, available resources and the volume of **Personal Data Processed** by us.

There are circumstances where access to data (whether considered **Personal Data** or not), that is stored on **TAQA Group** IT equipment provided to **TAQA Group Personnel**, would be required for document retrieval or investigation purposes. Such access can only be granted by the Head of **Ethics & Compliance Office** in writing, and in strict compliance with any directives issued. In addition, **Businesses** may not conduct their own document retrieval or investigations unless authorised by the Head of **Ethics & Compliance Office**.

2.7 Accountability

We are responsible for demonstrating our compliance with applicable **Data Protection Laws**. We demonstrate such compliance by outlining the steps we have taken to ensure the protection of the **Personal Data** that we **Process**, included in this Policy, and any other applicable data protection and data classification and retention policies.



2.8 Data Subject Rights

We **Process** all **Personal Data** in accordance with **Data Subjects**' rights under applicable **Data Protection Laws**. This may include complying with the below requests that we may receive from **Data Subjects**, although in some circumstances we will not, under **Data Protection Laws**, be required to meet the relevant **Data Subject's** request.

You must forward any requests received from **Data Subjects** to the **Ethics & Compliance Office**, who will consider the request in the context of the specific circumstances, before determining any appropriate actions to take.

(a) **Data Subject Access Requests**: **Data Subject** may submit requests to receive:

(i) Confirmation as to whether or not **Personal Data** relating to them is being **Processed**;

(ii) Information relating to how and why their **Personal Data** is being **Processed**; and

(iii) A copy of the **Personal Data** that we possess in relation to them.

(b) **Erasure and Rectification Requests: Data Subjects** may submit requests to correct inaccurate **Personal Data** that we hold about them, as well as requests to have all such **Personal Data** deleted. We will only erase such **Personal Data** so long as it is not in breach of local regulatory requirements.

(c) **Restriction Requests**: **Data Subjects** may submit requests that we cease **Processing** their **Personal Data** if they:

(i) Contest the accuracy of such data;

(ii) Believe the **Processing** is against the law;

(iii) Believe that we no longer require the **Personal Data** for the purpose for which it was collected; or

(iv) Object to the **Processing** of such data, and we verify whether there are legitimate grounds to **Process** such data which override the rights of the **Data Subject**.

(d) **Objections to Processing: Data Subjects** may submit objections to **Processing** conducted by us on the basis of legitimate business needs or for the performance of a task carried out on the basis of public interest.

(e) **Withdrawal of Consent**: Where we **Process Personal Data** on the basis of a **Data Subject's** consent, the **Data Subject** may withdraw its consent at a later time.

(f) **Data Portability Requests**: **Data Subjects** may submit requests to receive **Personal Data** which we hold about them in a structured, commonly used and machine-readable format, or to transmit such **Personal Data** to a third party.

2.9 Sharing Personal Data

(a) **General:** we may be required, in the course of our business, to share **Personal Data** that we hold with **Third Parties**. We will only share such **Personal Data** in compliance with applicable **Data Protection Laws**. Where we are required to do so by law, this may include sharing **Personal Data** with relevant law enforcement authorities and regulators.

(b) **International transfers:** Where we **Process Personal Data** we will comply with applicable restrictions in relation to the transfers of **Personal Data.** Data is subject to the laws and governance structures within the nation it is collected. We will only transfer **Personal Data** outside of the jurisdiction from which it originates:

(i) To countries determined by the applicable regulation as offering an 'adequate' level of protection; or

(ii) Where an appropriate safeguard is in place, including, among other things, standard contractual clauses, binding corporate rules, or in certain circumstances, where exceptions apply.

We should all consider the following questions before sharing any **Personal Data** with a third party, and you should contact the **Ethics & Compliance Office** if you are in any doubt as to whether the **Personal Data** concerned should be shared.

Determining what is Personal Data

Starting point

Are you able to identify a living individual from the Personal Data in your possession, or that is likely to come into your possession?

Yes | Not sure | No

01

Does the Personal Data relate to an identifiable living individual, whether relating to personal or family life, business, or profession?

Yes | Not sure

02

Does the information include a name, email address or identification/ reference number, or any information that may indirectly (alone or in combination with other identifiers) identify a Data Subject such as a phone number, physical address, online identifier, or online location data?

Yes | Not sure

03

Does the information reveal an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or health?

Yes | Not sure

The data is not Personal Data.

The data is Personal Data.

Contact the Ethics & Compliance Office for support via the Helpline (helpline.taqa.com).

3. ADDITIONAL POLICY REQUIREMENTS

- Vendors and Other Third Parties
- Automated Processing
- Privacy by Design and Privacy by Default
- Data Protection Impact Assessments (DPIA's)
- Keeping Written Records
- Personal Data Breaches
- Accountability, Training and Audit

3. Additional Policy Requirements

3.1 Vendors and Other Third Parties

(a) We will ensure that all vendors and other **Third Parties** that **Process Personal Data** on **TAQA Group's** behalf:

(ii) Are only given access to relevant **Personal Data**; and

(iii) Shall meet the requirements of **Data Protection Laws** when entering into written agreements with us that govern such **Processing** of **Personal Data**.

(b) We should include audit rights within our legal contracts to ensure compliance with these obligations and then exercise those rights as and when necessary.

3.2 Automated Processing

We will carry out a Data Protection Impact Assessment (**DPIA**) before any automated **Processing** or automated decision-making is carried out (see section 3.4 "Data Protection Impact Assessments (**DPIAs**)" for further information on **DPIAs**).

3.3 Privacy by Design and Privacy by Default

Privacy by Design and Privacy by Default are approaches to systems and process design which takes protection of **Personal Data** into account throughout the whole process and which is relevant to a range of circumstances including marketing permissions, employment on-boarding, and the sales process. We will implement Privacy by Design and Privacy by Default when **Processing Personal Data**, and in particular shall assess which measures shall be implemented on our programs, systems and processes.

3.4 Data Protection Impact Assessments (DPIA's)

(a) We will implement a **DPIA** (which will be reviewed by the **Ethics & Compliance Office**) as required by **Data Protection Laws**, before engaging in any "high risk **Processing**" (and in particular **Processing** using new technologies). In addition, we may have to consult with the **Supervisory Authority** before undertaking any high-risk **Processing**. A **DPIA** may also be required where there is a material change to an existing **Processing** activity.

(b) High-risk **Processing** may include:

(i) Evaluation or scoring, including profiling and predicting;

(ii) Automated decision-making with legal or similar significant effect;

(iii) Systematic monitoring;

(iv) **Processing** of **Special Category Data** or **Personal Data** of a highly personal nature;

(v) Large-scale **Processing**;

(vi) Matching or combining datasets;

(vii) **Processing** concerning vulnerable **Data Subjects**;

(viii) Innovative **Processing** or applying new technological or organizational solutions; and

(ix) Situations where the **Processing** in itself prevents **Data Subjects** from exercising a right or using a service or contract.

(c) A **DPIA** must include:

(i) A description of the **Processing**, its purposes and our legitimate business interests, if appropriate;

(ii) An assessment of the necessity and proportionality of the **Processing** in relation to its purpose;

(iii) An assessment of the risk to individuals; and

(iv) The risk mitigation measures in place and a demonstration of compliance.

(d) If you believe a **DPIA** may be required, you must consult the **Ethics & Compliance Office** as soon as possible using the Helpline (**helpline@taqa.com**) before **Processing** of the relevant **Personal Data** commences.

3.5 Keeping Written Records

We will maintain a written record of all **Processing** activities under our responsibility so that we comply with the requirements of applicable **Data Protection Laws**. This includes information about the purpose of the **Processing**, the categories of **Data Subject**, the categories of **Personal Data**, the categories of any recipients of the **Personal Data**, details of international transfers of **Personal Data**, the envisaged retention period applicable to **Personal Data**, and relevant security measures.

3.6 Personal Data Breaches

(a) We will comply with our obligations to notify any **Personal Data** breach to the **Supervisory Authority** and to the **Data Subject** as required by the applicable regulations.

(b) We will put in place procedures to deal with any suspected **Personal Data** breach, which shall include meeting our reporting obligations in a timely manner.

(c) You must report any actual or suspected **Personal Data** breach to the **Ethics & Compliance Office** as soon as possible.

3.7 Accountability, Training, and Audit

We will implement appropriate technical and organizational measures in an effective manner, to ensure compliance with **Data Protection Principles**.

We will have adequate resources and controls in place to ensure and document compliance with **Data Protection Laws**, including:

(a) Carrying out **DPIA's** where **Processing** presents a high risk to rights and freedoms of **Data Subjects**;

(b) Integrating data protection into internal documents including privacy procedures, related policies and standards, privacy notices, or fair processing notices;

(c) Regularly train you on **Data Protection Laws**, privacy procedures, related policies and standards and data protection matters including, for example, **Data Subjects'** rights, legal bases for **Processing**, **DPIA's**, and **Personal Data** breaches; and

(d) Regularly test the privacy measures implemented and conduct periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

4. FREQUENTLY ASKED QUESTIONS

4. Frequently Asked Questions

4.1 "I want to engage a third party to provide services in support of my team's work. Are there any Data Privacy considerations that I should take into account?"

*Where **Third Parties** provide us with services, we will often need to share some form of **Personal Data** with them to enable them to perform those services. **Data Protection Laws** require that we agree certain terms in writing to govern how the **Third Party** should **Process** this **Personal Data**. If any **Personal Data** is expected to be provided to the **Third Party**, you should work with the Legal Department to ensure that your contract contains the necessary provisions relating to data protection.*

4.2 "I've sent an email that had an unencrypted file attached containing HR Personal Data to the wrong recipient. Is that a problem?"

*This may constitute a 'data breach'. Under **Data Protection Laws**, we may be required to report such an incident to the relevant regulatory authorities, as well as the affected individuals. You should notify the **Ethics & Compliance Office** of any actual or suspected data breach as soon as possible after becoming aware of it, so they can determine the appropriate next steps without delay.*

4.3 "I plan to use a new piece of software to help me save time analyzing some information containing customer Personal Data. Do I need to carry out a DPIA?"

DPIA's *need to be carried out whenever we engage in 'high risk* ***Processing****'. Whether* ***Processing*** *falls into this category will need to be considered on a case-by-case basis, but applying new technological or organizational solutions will generally constitute 'high risk* ***Processing****'. Therefore, a* ***DPIA*** *would be required in this instance. You should make yourself familiar with the guidance in this Data Protection Policy on* ***DPIA's****, and if you're unsure if one is required, check with the* ***Ethics & Compliance Office****.*

4.4 "I've received an email from a **Data Subject** asking me to send them copies of all **Personal Data** relating to them that we have on file. Should I comply with their request?"

Data Subjects *have various rights under* ***Data Protection Laws****, which include the right to make 'access requests' like this to organizations that* ***Process*** *their* ***Personal Data****. However, the rules surrounding these requests, and if and how we should comply with them, are complex. Where we do comply with such a request, we need to be mindful of issues like disclosing* ***Personal Data*** *of other* ***Data Subjects*** *at the same time. Accordingly, you should forward any such requests to the* ***Ethics & Compliance Office****, who will determine the appropriate course of action.*

BUSINESS PARTNER DUE DILIGENCE POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

Implementation of this Policy

1. Policy Summary

1.1 Summary

(a) We are committed to conducting our business in accordance with the highest ethical standards. We have a zero-tolerance approach to any form of unethical or illegal behavior and to any breaches of the laws that govern **Bribery**, **Corruption**, **Money Laundering**, **Counter Terrorist Financing**, **Sanctions**, and **Trade Controls**.

(b) Conducting **Due Diligence** on our **Business Partners** is a critical part of ensuring that we are compliant with those laws in order to protect our reputation. The conduct of our **Business Partners** can have serious implications for the **TAQA Group**, both ethically and legally. It is essential that we perform appropriate, risk-based **Due Diligence** on potential **Business Partners** prior to doing business with them, as well as throughout our business relationship with them.

(c) Each **Business** is responsible for ensuring that the requirements of this Policy are met and must establish the level of **Due Diligence** appropriate to that **Business**. Establishing the appropriate level of **Due Diligence** will depend on a wide range of factors. This Policy sets out the minimum standards required for **Due Diligence** and provides guidance on the relevant principles. In the absence of a comprehensive **Due Diligence** process available to you at your **Business** that meets the requirements of this Policy, you should use the **Business Partner Risk Assessment Score Sheet** (Steps 1 – 7), also available on the **Ethics & Compliance Office** Homepage of the Intranet to help conduct your **Business Partner Risk Assessment**.

(d) This Policy supports our **Sanctions and Trade Controls Policy**, **Anti-Money Laundering Policy**, **Anti-Bribery & Corruption and Anti-Fraud Policy**, **Code of Ethics & Business Conduct**, and **Busswiness Partner Code of Conduct**. You should refer to those policies where appropriate to understand the background to the requirements in this Policy.

(e) You should ensure that all **Business Partner** confirm that they will abide by our **Business Partner Code of Conduct** and the principles of our **Code of Ethics & Business Conduct**.

(f) All legal agreements with **Business Partner** must only allow for subcontracting where **TAQA Group** has given prior written approval.

(g) If you have any doubts, questions, or concerns about this Policy you should contact the **Ethics & Compliance Office** on the Helpline (**helpline.taqa.com**).

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability, and reputational damage. You may also be subject to disciplinary action, including but not limited to termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics and Business Conduct** and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office.**

(c) Complete the annual training associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations, you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

1.5 Implementation of this Policy

(a) Each **Business** is responsible for implementing this Policy, ensuring that appropriate **Due Diligence** procedures are put in place. As a minimum, all requirements provided within this Policy must be met in relation to **Business Partner Due Diligence**.

(b) The diagram below sets out a summary of the minimum level of **Due Diligence** required prior to formalizing any relationship with a potential **Business Partner**.

2. PROCESS IN SUMMARY

2. Process In Summary

01

Identify and Classify

Business Partner

- Partner
- Agent
- Contractor
- Consultant
- Supplier/Vendor
- Customer
- M&A* Target
- Other

Assign the applicable risk score according to services provided or role played.

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 1.

**M&A: Merger and Acquisition*

02

Know

YOUR BUSINESS PARTNER

- Obtain required KYC** information
- Obtain a Credit Record Check (where relevant).
- Understand Business Partner's History
- Know Business Partner's Source of Funds
- Verify Identity and Ownership

If you are using the Business Partner Risk Score Sheet, send out the Business Partner Information Form for your Business Partner to complete.

***KYC: Know Your Customer*

03

Sanctions Screening

Screen the following:

(a) Business Partner;

(b) Business Partner's Directors; and

(c) Business Partner's Owners.

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 3.

04

Red Flag Review

Are any red flags present?

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 4.

05

Geographic Check

Check the following lists:

(a) Corruption Perceptions Index;

(b) Basel AML Index; and

(c) List of EU list of non-cooperative jurisdictions.

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 5.

06

Industry Check

Check industry risk

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 6.

07

Contract Value Check

Assign score according to contract value

If you are using the Business Partner Risk Score Sheet calculate the risk score in accordance with step 7.

08

Overall Risk Classification

If you are using the Business Partner Risk Score Sheet determine the overall risk classification by adding the individual scores for each of the factors mentioned above.

Next Steps

Take appropriate action in accordance with section 3.4

You may need to undertake Enhanced Due Diligence and contact the Ethics & Compliance Office and the Legal Department

3. DUE DILIGENCE PROCESS

- Step 1: Identify your Business Partner
- Step 2: Know Your Business Partners
- Steps 3-8: Sanctions Screening and Risk Assessment
- Step 9: Overall Risk Classification
- Enhanced Due Diligence
- Formalizing Your Relationship
- Ongoing Monitoring
- Auditing

3. Due Diligence Process

In the absence of a comprehensive Due Diligence process available to you at your Business (that meets the requirements of this Policy), you should use the Business Partner Risk Assessment Score Sheet (Steps 1 – 7), also available on the Ethics & Compliance Office Homepage of the Intranet to help conduct your Business Partner Risk.

3.1 Step 1: Identify your Business Partner Type

A **Business Partner** is, in essence, any person or organization that we do business with. A range of third parties can potentially be **Business Partners**.

Different Types of Business Partners:

- **Partner**: An individual or organization that has entered into a business relationship with TAQA Group (e.g. to establish a new joint business entity/arrangement, manage assets or otherwise pool resources).
- **Agent**: An individual or organization authorized to act for, or on behalf of, TAQA Group.
- **Contractor**: An individual or organization that provides goods or services to TAQA Group. The contractor may hire a sub-contractor to perform specific tasks, where approved by TAQA Group and for the purposes of this Policy, the term Contractor includes any duly appointed sub-contractors.
- **Supplier/vendor**: An individual or organization that supplies products or services to **TAQA Group**.
- **Consultant/advisor:** An individual or organization providing services and/or advice to **TAQA Group** (e.g. legal, tax, accountancy or financial advisors/consultants).
- **Customer:** The recipient of a product or service supplied by the **TAQA Group**.
- **M&A Target:** An organization or entity that **TAQA Group** is undertaking **Due Diligence** on with a view to a potential merger or acquisition.

Although this Policy does not apply to **Retail Customers**, to the extent that a **Retail Customer** is also a **Business Partner**, then this Policy will be applicable.

All legal agreements with **Business Partners** must only allow for subcontracting where **TAQA Group** has given prior written approval. If a **Business Partner** seeks approval for the use of a subcontractor, approval should only be given subject to a contractual requirement for the **Business Partner** to undertake appropriate **Due Diligence** on such subcontractor in accordance with the minimum standards as set out in this Policy. Any approved subcontractor must also confirm that they will abide by our **Business Partner Code of Conduct** and the principles of our **Code of Ethics & Business Conduct**.

This Policy sets out processes in respect of assessing **M&A Targets** from a risk management perspective. However, **TAQA Group's** legal and corporate due diligence processes for potential **M&A Targets** are subject to separate procedures. The Policy is not intended to comprehensively or exhaustively address the risks and specific **Due Diligence** associated with any mergers and acquisitions that the **TAQA Group** may undertake. Such risks must be considered on a deal-by-deal basis in collaboration with the **Ethics & Compliance Office** and the Legal Department.

The role of the **Business Partner** and the services (if any) that they would provide for **TAQA Group** influences the level of risk that may be associated with such **Business Partner**. The sliding scale below indicates the general level of risk associated with **Business Partners**:

If you are using the Business Partner Risk Assessment Score Sheet as part of your **Due Diligence**, complete Step 1 of the **Business Partner Risk Assessment Score Sheet** by assigning the **Business Partner** a score depending on the classification of their role and services, as specified in Step 1 of the **Business Partner Risk Assessment Score Sheet**.

3.2 Step 2: Know Your Business Partners

A knowledge and understanding of our **Business Partners** is key to helping us address legal and commercial risks. We should not conduct business with an anonymous or fictitious company or with any **Business Partners** with an unclear identity or business activities.

As such, you must ensure that an appropriate level of **KYC** checks on potential **Business Partners** is carried out before entering into any business arrangement with them. The minimum information required is summarized below, and fully set out in the Business Partner Information Form which can be found in Step 2 of the **Business Partners Risk Score Sheet**, also found on the **Ethics & Compliance Office** Homepage of the Intranet. In the absence of an alternative due diligence information form, you should send this Business Partner Information Form to your **Business Partner** for completion.

The following steps are the minimum **KYC** checks that should be undertaken in all cases:

Obtain key company information from your potential **Business Partner**, including:

- Company name, parent company details (if applicable), company registration number, tax number, and website URL;
- Registered office address and head office address (if applicable);
- A copy of the certificate of incorporation (if applicable);
- An official extract of the register of companies (or equivalent) (if applicable);
- The articles of association and other company constitutional documents (if applicable);
- Names of Directors (if applicable);
- Contact details of the person who is your focal point of contact;
- The list of people authorized to sign on behalf of the company and corporate documents/powers of attorney confirming those rights (if applicable and please note that in certain cases it may be more appropriate to seek this information upon contract signing);
- Where possible, the last 2 years' worth of financial statements and audit reports (cash flow, balance sheet, and profit & loss account);
- Payment address/purchase ordering address if different to head office address;
- Payment details, including the full name and address of the **Business Partner's** bank, as well as their account details; and
- A confirmation on behalf of the **Business Partner** that all the information required above is correct and accurate.

Once you have obtained the key company information, you should:

- Know and verify the true identity of the **Business Partner** using reliable sources, documents, data or information;
- If your **Business Partner** is a company, identify and verify the beneficial owners of the **Business Partner** who have more than a 10% legal or beneficial ownership interest in the **Business Partner**;
- Check whether any of your **Business Partner**'s owners, **Directors**, or officers, are **Public Officials**.
- Run a credit record check (or equivalent) on the **Business Partner** (where relevant - i.e. as part of **Enhanced Due Diligence** – see below);
- Be familiar with the nature and history of the **Business Partner's** activities (to the extent possible); and
- Identify the **Business Partner's** source of, or use of, funds.

Once this information has been obtained from the potential **Business Partner**, it must be kept along with any other evidence gathered, in accordance with the applicable document retention requirements (please see the **Data Privacy Policy** for further detail of such requirements).

In order to complete the initial **Due Diligence** on your **Business Partner** you will need additional information which could be available through an internet search. However, an internet search does not negate the need for you to carry out a screening search using any available third-party screening tool within your **Business.**

An internet search may also help to identify whether the **Business Partner** has any links to **Sanctioned Countries** and **Sanctioned Persons**, as well as any other red flags (see section 3.3, steps 3 and 4 below), such as unfavorable news articles or press reports indicating potentially corrupt unethical or illegal behaviors.

In the absence of an alternative due diligence checklist available to you at your **Business** that meets the requirements of this Policy, all **KYC** steps taken and information gathered about your **Business Partner** must be recorded using the Business Partner Information Checklist embedded in Step 2 of the **Business Partner Risk Assessment Score Sheet**, also found on the **Ethics & Compliance Office** Homepage of the Intranet.

If there are any questions about the information checks or any suspected red flags at this initial **KYC** stage, the **Ethics & Compliance Office** or Legal Department should be contacted for guidance.

3.3 Steps 3 - 7: Sanctions Screening and Business Partner Risk Assessment

Overview

Sanctions Screening and a **Business Partner Risk Assessment** must be undertaken on all potential **Business Partners** to ensure that we are conducting our business lawfully and not breaching **Sanctions**, and to ensure to the extent possible that a potential **Business Partner** does not pose a serious risk to **TAQA Group**.

This process will establish whether you must contact the **Ethics & Compliance Office** and the Legal Department prior to starting or continuing the relationship and whether or not **Enhanced Due Diligence** should be conducted.

A written record of the steps taken in assessing the risks associated with the potential **Business Partner** must be retained either through the completion of Steps 1 to 7 of the **Business Partner Risk Assessment Score Sheet** also found on the **Ethics & Compliance Office** Homepage of the Intranet, or by using the alternative written record available to you at your **Business**.

Although not exhaustive, the factors below must be considered when assessing the level of risk posed by a potential **Business Partner**:

Step 3 - Sanctions:

if the potential **Business Partner** (or its beneficial owners or directors) are considered a **Sanctioned Person** or has links to a **Sanctioned Country**.

***Step 4 - Red flags*:** anything unusual, suspicious or otherwise different about the potential **Business Partner** and/or the underlying transaction that could give rise to **Money Laundering**, **Terrorist Financing**, **Bribery**, and/or **Corruption**-related concerns.

***Step 5 - Geography*:** the potential **Business Partner** is based in, or the underlying transaction is otherwise connected to, a country that is perceived as being of higher risk from a **Bribery** and **Corruption**, **Money Laundering**, **Terrorist Financing** and/or tax compliance perspective.

Step 6 - Industry: the potential **Business Partner** operates in an industry that is perceived as being higher risk.

***Step 7 - Contract value*:** the expected value of the contract opportunity. We require that greater scrutiny is applied to all high value contracts.

Further guidance on these points is set out below.

In the following sub-sections, we set out a number of factors to be considered in order to evaluate the level of risk posed by each potential **Business Partner** and to establish whether approval from the **Ethics & Compliance Office** is required and what degree of **Due Diligence** should be undertaken, including whether **Enhanced Due Diligence** should be conducted.

The **Business Partner Risk Assessment Score Sheet** attributes each factor with a risk score depending on the risks that may be applicable to your **Business Partner**. When evaluating a potential **Business Partner**, you must add the scores assigned to each factor in order to generate an overall risk score for the potential **Business Partner** - Step 8 of the **Business Partner Risk Assessment Score Sheet**.

Step 3: Sanctions Screening

Sanctions Screening should be carried out in order to check whether a **Business Partner** is a **Sanctioned Person** or is linked to a **Sanctioned Country**.

In general terms, a **Sanctioned Person** is a person located or incorporated in a **Sanctioned Country** or targeted by **Sanctions** issued by governments from time to time. Please also refer to the **Sanctions and Trade Controls Policy** for further guidance.

Sanctions Screen the following people and entities to find out if they are a **Sanctioned Person** or are linked to a **Sanctioned Country:**

(a) Your **Business Partner**;

(b) Any of your **Business Partner's Directors** and officers who you have identified, if your **Business Partner** is a company; and

(c) If your **Business Partner** is a company, any owners you have identified.

Your **Sanctions Screening** should be conducted through an internet search together with any third-party **Business** screening tool you have access to, and an analysis of the **KYC** information you have received. If you have any questions or concerns regarding any third-party screening tool being used by your **Business**, please contact the Legal Department or the **Ethics & Compliance Office**.

The results of these checks will indicate if any of the people and entities that you have screened are a **Sanctioned Person** or linked to a **Sanctioned Country**.

A written record of the outcome of your **Sanctions Screening** must be retained.

In the event that a potential **Business Partner** is a **Sanctioned Person** or is linked to a **Sanctioned Country**, written approval of the Legal Department and the **Ethics & Compliance Office** must be obtained prior to starting or continuing the relationship.

Step 4: Bribery and Corruption Red Flag Review

Bribery and **Corruption** come in many different forms and further background information can be found in the **Anti-Bribery & Corruption and Anti-Fraud Policy**. We must be alert to the possibility that the relationships that we are entering into could be connected to unlawful or unethical behaviors.

Where we are aware of anything unusual or suspicious about the **Business Partner** and/or the underlying transaction, which could give rise to **Bribery** and **Corruption**-related concerns, we should treat this as a red flag.

A list of red flags that you are expected to take into account is set out below. If you are using the **Business Partner Risk Assessment Score Sheet**, you must assign each potential **Business Partner** an overall red flag risk score as provided in Step 4 of the **Business Partner Risk Assessment Score Sheet**.

Remember that these potential red flags are not exhaustive. Be alert to any other facts or circumstances that may suggest that the contract or transactions with the **Business Partner** are not typical or otherwise in the ordinary course of **TAQA Group's** business. If you are aware, or become aware of, any facts or circumstances that you consider should be treated as a red flag but are not listed below, please contact the **Ethics & Compliance Office** for further guidance.

By way of example, if a potential **Business Partner** has an unclear ownership structure and is suggesting that no written agreement be put in place, these are red flags.

Red Flags

- The **Business Partner** proposes to give gifts or provide entertainment/business meals to a Third Party above the value threshold of US$150 / AED 550.
- The **Business Partner's** fees are unusually high for their services, or fee arrangements are not transparent or are otherwise unusual.
- The **Business Partner** has an unclear ownership structure or lacks a clear office or work address.
- **Public Officials** or **Politically Exposed Persons** are (directly or indirectly) involved with the transaction or relationship.
- The **Business Partner** relies heavily on contacts rather than expertise in order to win business.
- There is a reputation of **Bribery** or **Corruption** in the proposed **Business Partner's** organization (including it having been subject to a regulatory investigation or prosecution) or any adverse coverage about the **Business Partner's** reputation, qualifications or trustworthiness (and this extends to any personnel, including directors, within the organization).
- The **Business Partner** is suggesting that no written agreement relating to the business is put in place.
- The **Business Partner** seeks payment to be made in an unusual or non-transparent manner. For example, where payment is requested to be made to a **Third Party** other than such **Business Partner**.
- There is no valid commercial justification for the use of the **Business Partner**.
- There is a lack of visibility about the **Business Partner's** services or how it operates (e.g. if there is no obvious record of it doing business).
- The **Business Partner** makes any of the following demands: payments of commission to other **Third Parties**; payments of commission in cash or other untraceable funds; and/or payments of commission into foreign bank accounts or to unidentifiable companies.
- The **Business Partner** refuses to provide requested screening information or to include any anti-**Bribery** and **Corruption**-related legal provisions in a resulting contract.
- The **Business Partner** has an apparent lack of qualifications or resources needed to perform the services they are offering.
- Behavior of any kind that would be prohibited by the **Code of Ethics and Business Conduct** (including human rights violations and any abuse to the environment), **Anti-Money Laundering Policy**, the **Sanctions and Trade Controls Policy** or the **Anti-Bribery & Corruption and Anti-Fraud Policy**, if undertaken by **TAQA Personnel**.

Step 5: Geography Check

Certain locations and countries are considered to be higher risk than others and therefore **Bribery** and **Corruption** are perceived as being more likely to occur, or because they are considered a higher risk from a **Money Laundering**, **Terrorist Financing** and/or tax compliance perspective.

The "Corruption Perceptions Index" (available at: **www.transparency.org/en/**) ranks 180 countries and territories by their perceived levels of public sector corruption, according to experts, with a score from 1 to 100.

The "Basel AML Index" (available at: **www.baselgovernance.org/basel-aml-index**) ranks 125 countries according to their risk of money laundering and terrorist financing.

You must assess the risk that is associated with your **Business Partner's** country. If you are using the **Business Partner Risk Score Sheet**, you must assign the **Business Partner** a score in Step 5 of the **Business Partner Risk Assessment Score Sheet** depending on where the **Business Partner** is located, in accordance with the country's ranking on the latest published "Corruption Perceptions Index" and the "Basel AML Index".

Notwithstanding the above, if the potential **Business Partner** is located in a country or territory listed in the "EU list of non-cooperative jurisdictions", the potential **Business Partner** must automatically be given a higher risk score. This is because such jurisdictions are considered higher risk from a tax compliance perspective. You can find the "EU list of non-cooperative jurisdictions" (available at **www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/**).

Step 6 - Industry Check

The type of industry that a **Business Partner** operates within influences the level of risk that may be associated with such **Business Partners**. Transparency International's "Bribe Payers Index" (available at **www.transparency.org/en/**) sets out perceptions of **Bribery** across business sectors including "private to private" **Bribery** between companies.

You must assess the risk that is associated with your **Business Partner's** industry. If you are using the **Business Partner Risk Score Sheet**, you must assign the **Business Partner** a score in Step 6 of the **Business Partner Risk Assessment Score Sheet** depending on the industry the **Business Partner** operates within.

Step 7: Contract Value Check

Higher value contracts can be considered to be more exposed to **Bribery** and **Corruption**-related risks and thus subject to further scrutiny by regulators and enforcement agencies.

Bribery and **Corruption** issues regarding key **Business Partners** could also present a significant risk to **TAQA Group**'s overall reputation and credibility.

For these reasons, we require that higher standards of **Due Diligence** are applied to higher value contracts. If you are using the **Business Partner Risk Score Sheet**, you must assign the **Business Partner** a score in Step 7 of the **Business Partner Risk Assessment Score Sheet** depending on the value of the proposed contract.

In assessing the value of the contract, you should have regard to the following principles:

(a) Framework Agreements or Master Service Agreements (e.g. for recurring engagements): the appropriate contract value threshold will be determined by considering all expected or reasonably anticipated underlying contracts giving rise to revenues for either **TAQA Group** or the **Business Partner**; and

(b) Series of Contracts: where, in any given 12-month period, you become aware that **TAQA Group** has entered into a series of contracts each with revenues less than a certain value threshold, but which collectively provide cumulative revenues in excess of a value threshold for either **TAQA Group** or the **Business Partner**.

3.4 Step 8: Overall Risk Classification

Upon completion of your **Due Diligence** on your **Business Partner**, you must assign an **Overall Risk Classification** that will guide you as to whether there are any further due diligence steps that need to be taken, such as **Enhanced Due Diligence**. The table below sets out the **Overall Risk Classification** brackets. Depending on what level of risk the **Business Partner** poses, you must take the relevant next steps outlined in the table below and ensure that they are recorded in the **Business's Books and Records**.

If you have used the **Business Partner Risk Assessment Score Sheet** you should now complete the **Overall Risk Classification** in Step 8 of the **Business Partner Risk Assessment Score Sheet**. This will involve adding the individual scores for each of the factors mentioned above in order to determine an overall risk classification for the proposed **Business Partner**. This will determine what further steps (if any) you must take before engaging with the proposed **Business Partner**.

Overall Risk Classification	Next Steps
Low Risk	Record the steps taken in the assessment and **KYC** checks. No further action needed.
Medium Risk	Record the steps taken in the assessment and consider what risk management steps may still be required (if any). For example, it may be necessary to conduct further due diligence on the **Business Partner** and/or secure contractual protections from them.
High Risk	Record the steps taken in the assessment and consider what risk management steps may still be required (if any). For example, it may be necessary to secure contractual protections from the **Business Partner**. **Enhanced Due Diligence** should be conducted.
Highest Risk	Prior written approval of the **Ethics & Compliance Office** and the Legal Department is required before entering into this relationship. **Enhanced Due Diligence** should be conducted in coordination with the **Ethics & Compliance Office** and the Legal Department.

3.5 Enhanced Due Diligence

Once the **Overall Risk Classification** is complete, **Enhanced Due Diligence** may be required. Note that you should also complete this **Enhanced Due Diligence** if any screening tool you have access to indicates that you should do so.

Typically, the **Enhanced Due Diligence** will involve some or all of the following additional steps. However, the required steps will depend on the nature and extent of the risks identified:

(a) Request that the potential **Business Partner** provides additional information to address the specific issues of concern;

(b) In the case of a company, obtain its full corporate profile and history;

(c) In the case of a person, obtain their full employment history and request character and professional references;

(d) Undertake litigation and criminal records searches which may be available to you through a screening tool or service;

(e) Where appropriate, contact trusted third party **Business Partners** and other sources in the same sector or geography to seek their views;

(f) Conduct appropriate checks to validate the financial strength of the **Business Partner**. For example, through use of independent tools to check whether the **Business Partner's** credit score is adequate (where relevant); and

(g) Consider holding in-person site visits and/or interviews with the potential **Business Partner**.

The **Ethics & Compliance Office** and the Legal Department should be contacted if specialist assistance with **Enhanced Due Diligence** is required.

3.6 Formalizing Your Relationship

Once the **KYC** checks and any **Due Diligence** has been completed, the relationship with the **Business Partner** can be formalized. All relationships should be documented through a formal written legal agreement and you should ensure that **Business Partners** are supplied with a copy of our **Business Partner Code of Conduct** and agree to abide by its terms.

The Legal Department should advise on any particular contractual terms that are appropriate in the light of the outcome of the **Due Diligence** process on the **Business Partner**.

3.7 Ongoing Monitoring

We must remain aware of the risks associated with our **Business Partners** and, where necessary, undertake periodic checks to ensure that the risks have not changed.

Where a new red flag is identified and prior to any renewal of your relationship with your **Business Partner** or where new or additional services will be provided, a reassessment of the **Business Partner** must be undertaken.

3.8 Auditing

If the relationship with a **Business Partner** includes audit rights, those rights should be exercised.

An appropriate audit schedule for routine audits should be agreed with the **Business Partner**. Any red flags may indicate the need for a non-routine audit to take place.

The **Ethics & Compliance Office** in conjunction with Internal Audit may conduct periodic checks on **Businesses** to ensure compliance with this Policy so it is important to ensure that all relevant records are maintained.

4. FREQUENTLY ASKED QUESTIONS

4. Frequently Asked Questions

4.1 "I'm concerned because a potential supplier is located in a **Sanctioned Country**. What should I do?"

*As the country where the supplier is located is a **Sanctioned Country**, you will need to obtain the prior written approval of both the **Ethics & Compliance Office** and Legal Department before you can enter into a business relationship or transaction with them.*

4.2 "There has been a change to one of the **Directors** of our **Business Partner** and I suspect he may be targeted by **Sanctions**. Do I need to take any further steps?"

*On-going monitoring of **Business Partners** is an important part of **Business Partner Due Diligence**. If there is a change of **Director**, you should run additional **Sanctions Screening** on the new **Director**. The results of the checks will indicate if the **Director** is a **Sanctioned Person**. If there is a potential **Sanctions** concern, you should discuss with the **Ethics & Compliance Office** and Legal Department immediately.*

4.3 "One of the owners of a potential customer is listed on a US sanctions list. Does this matter?"

*Yes, **Sanctions** restrictions can sometimes be triggered if an owner of the **Business Partner** is a **Sanctioned Person**. US sanctions can also have a very broad reach and can impact on **TAQA Group's** operations outside of the US. You will need to obtain the prior written approval of the **Ethics & Compliance Office** and Legal Department before you could enter into a business relationship or transaction with this **Business Partner**.*

4.4 "A prospective customer is located in a country that received a score of 30/100 on the Transparency International "Corruption Perceptions Index". Does this mean we cannot work with them?"

*Not necessarily. As the **Business Partner** is located in a higher risk country, **Enhanced Due Diligence** may be required in order to gain additional comfort and assurance that the **Business Partner** does not pose an undue risk to **TAQA Group**. This will also depend on the other risks associated with the **Business Partner**.*

4.5 "I have seen a media report that a potential contractor has a previous bribery-related conviction. What should I do?"

*This is useful information and raises a red flag. You should conduct further **Due Diligence** and seek to find out further information. Depending on the overall risk score associated with the **Business Partner**, you may also need to conduct **Enhanced Due Diligence** and/or notify the **Ethics & Compliance Office** and the Legal Department, so that they can advise on what further steps to take.*

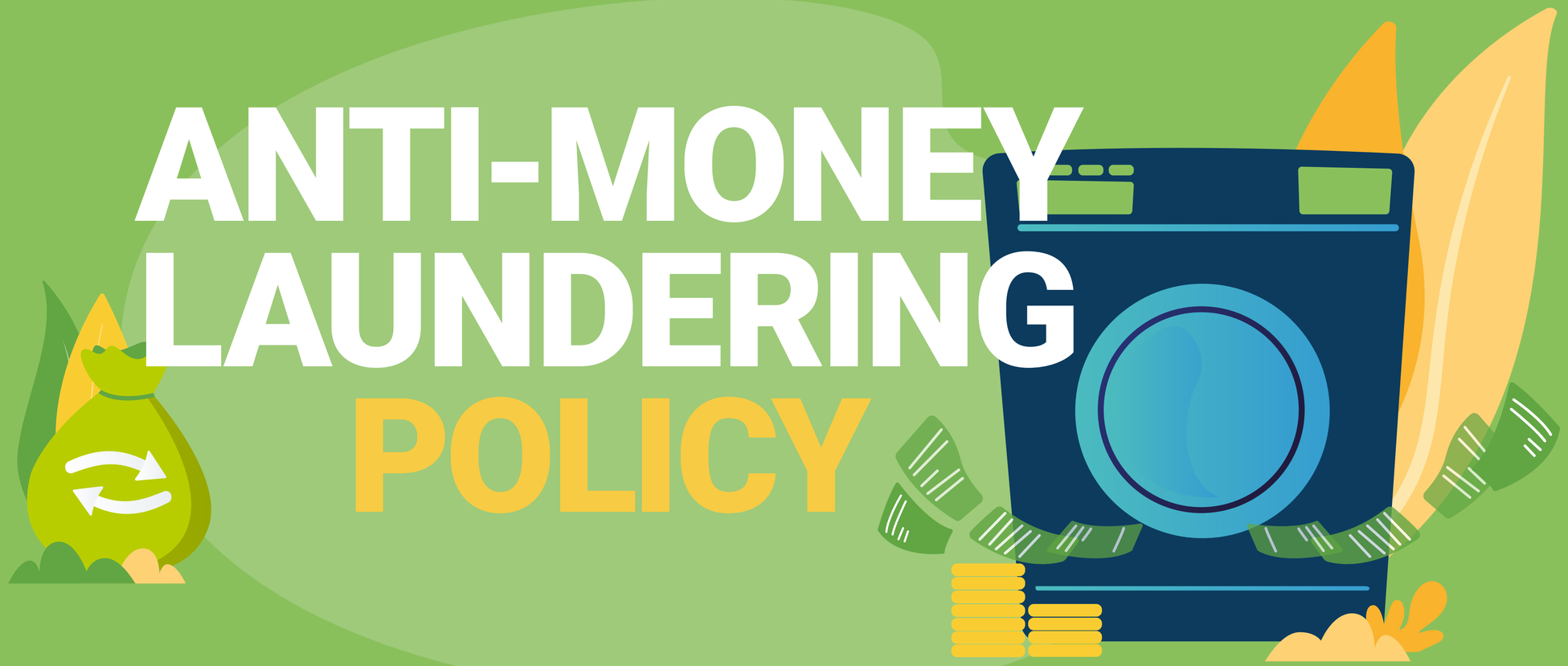
4.6 "A distributor located in Dubai has asked us to send payment to a firm registered in the Cayman Islands. Our business with this distributor doesn't involve the Cayman Islands. Should I be concerned?"

*Requesting that payments be made to a jurisdiction that is not related to the transaction is a red flag and further **Due Diligence** should be conducted to find out why the distributor is requesting that the payment be made to an entity in the Cayman Islands. Depending on the overall risk score associated with the **Business Partner**, you may also need to conduct **Enhanced Due Diligence** and/or notify the **Ethics & Compliance Office** and the Legal Department, so that they can advise on what further steps to take.*

4.7 "A supplier is refusing to provide information to confirm their identity. Is this an issue?"

*It is important to verify the identity of the **Business Partner** so that we can be sure they are not fictitious and do not create a **Money Laundering**-related risk. If the **Business Partner** continues to refuse, depending on the **Business Partner's** overall risk score, you should, at the very least, conduct **Enhanced Due Diligence** on the **Business Partner** and consult with the **Ethics & Compliance Office** and the Legal Department.*

ANTI-MONEY LAUNDERING POLICY



1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

1. Policy Summary

1.1 Summary

(a) **Money Laundering** and **Terrorist Financing** are very serious criminal offences. We are committed to conducting our business in accordance with the highest ethical standards and have a zero-tolerance approach to **Money Laundering** and **Terrorist Financing**.

(b) This Policy sets out guidance on how to identify and prevent **Money Laundering** and **Terrorist Financing**.

(c) This Policy is not intended to prevent legitimate activities directly related to the conduct of **TAQA Group's** business.

(d) If you have any doubts, questions or concerns about this Policy you should contact the **Ethics & Compliance Office** on the Helpline (**helpline.taqa.com**).

(e) You must:

(i) Not engage in or facilitate any **Money Laundering** or **Terrorist Financing**;

(ii) Be aware of **Money Laundering** or **Terrorist Financing** risks and report any concerns;

(iii) Not tip off an individual in respect of, or compromise, an investigation into known or suspected acts of **Money Laundering** or **Terrorist Financing**;

(iv) Understand the internal controls and procedures in the **Business** that you work for;

(v) Conduct appropriate **Due Diligence** on **Business Partners** in accordance with the terms of the **Business Partner Due Diligence Policy** and be aware of any **Money Laundering** or **Terrorist Financing**-related red flags; and

(vi) Keep accurate **Books and Records**.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues and **TAQA Group** at risk of civil and/or criminal liability, and reputational damage. You may also be subject to disciplinary action, up to and including termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office**.

(c) Complete any training associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

2. POLICY REQUIREMENTS

- Money Laundering and Terrorist Financing
- Business Partners
- Books and Records

2. Policy Requirements

2.1 Money Laundering and Terrorist Financing

Money Laundering takes many forms. In simple terms, it involves turning "dirty" money (i.e. money earned in the course of an illegal or criminal activity) into "clean" money (i.e. money which cannot be traced back to illegal or criminal activity) by using it in such a way that it is no longer apparent that it relates to, or is the product of, crime or criminal conduct.

Terrorist Financing relates to the financing of terrorist acts, terrorists, and terrorist or illegal organizations.

Money Laundering or **Terrorist Financing** are criminal offences in the jurisdictions in which **TAQA Group** operates. Any involvement in **Money Laundering** or **Terrorist Financing** is illegal including:

(a) Concealing, disguising, converting, handling, collecting, preparing, moving, providing, or transferring criminal or terrorist property;

(b) Removing criminal or terrorist property from a country;

(c) Entering into, or becoming concerned with, an arrangement that helps with the purchase, possession, use or control of criminal or terrorist property;

(d) Acquiring, using, and/or possessing criminal or terrorist property;

(e) Financing terrorist acts, terrorists and terrorist organizations and other criminal activity;

(f) Failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in **Money Laundering** or **Terrorist Financing**; and

(g) Tipping off an individual in respect of or, compromising an investigation into known or suspected acts of **Money Laundering** or **Terrorist Financing**.

So, you must:

(a) Not engage in or help with any **Money Laundering** or **Terrorist Financing**;

(b) Be aware of **Money Laundering** or **Terrorist Financing** risks and report any concerns;

(c) Not tip off an individual in respect of, or compromise an investigation into acts of known or suspected **Money Laundering** or **Terrorist Financing**; and

(d) Understand the internal controls and procedures in the **Business** that you work for.

Set out below are some examples of **Money Laundering** or **Terrorist Financing.**

Examples:

- You purchase an item from a **Business Partner** when you know that the item is stolen.
- You allow a **Business Partner** to pay **TAQA Group** for goods or services using funds derived from criminal activities.
- You help a **Business Partner** transport stolen goods out of a country under **TAQA Group's** name.
- You give money to a **Business Partner** knowing or suspecting that they will use it to help pay for a terrorist act.
- You hold or transfer funds resulting from a criminal act.

2.2 Business Partners

Understanding and managing our **Business Partners** is key to helping us to address **Money Laundering** and **Terrorist Financing** risks.

You must:

(a) Conduct appropriate risk-based **Due Diligence** on **Business Partners** and exercise ongoing monitoring of them. Please refer to the **Business Partner Due Diligence Policy** for further information and requirements;

(b) Include appropriate terms in contracts with and/or obtain confirmation from **Business Partners** that commit them to comply with applicable **AML** and **CTF** laws; and

(c) Provide all **Business Partners** with the **Business Partner Code of Conduct**.

We cannot list all of the issues that may be red flags and could give rise to knowledge or suspicions in respect of **AML** and **CTF** laws. You should be vigilant and consider each case individually. However, the following examples may assist you.

Examples:

- Your **Business Partner** is reluctant, or refuses, to provide necessary contact personal details as required in the context of the transaction, business background information, or verifiable documentation as proof of its identity.
- Your **Business Partner** requests funds to be refunded to them in cash on a regular basis.
- Your **Business Partner** is a **Politically Exposed Person** or a transaction involves a **Politically Exposed Person**.
- Your **Business Partner** wants to make or receive a large cash payment.
- Your **Business Partner** wants you to pay funds to a bank account that is in a different country from their own country of residence, or to an account registered to an unrelated entity.
- Transactions with your **Business Partner** are not typical, appear to have no economic justification or are substantially different from past transactions with such counterparty.
- There are media reports that your **Business Partner** is engaged in criminal activity.
- Your **Business Partner** has links to terrorists or terrorist organizations.

2.3 Books and Records

TAQA Group must keep accurate **Books and Records** that record our decisions and why we made them, and reflect transactions and our assets in reasonable detail, supported by a proper system of internal accounting controls.

To enable this, you must:

(a) Follow our standard accounting rules and procedures. “Off-the-book” accounts and false or deceptive entries in our **Books and Records** are unacceptable, and could expose you to disciplinary action including, but not limited to, termination of employment;

(b) Document, review, and properly account for all financial transactions in the **Books and Records** of the relevant **Business**;

(c) Follow all relevant financial controls and approval procedures; and

(d) Retain and archive the records of the relevant **Business** in accordance with company standards, and other applicable laws and regulations (including those relating to tax).

3. FREQUENTLY ASKED QUESTIONS

3. Frequently Asked Questions

3.1 "Should I be concerned if a **Business Partner** repeatedly refuses to share basic details about their business?"

*"If a **Business Partner** is reluctant to disclose basic details concerning their business this is a red flag and could suggest that they are engaged in **Money Laundering** or **Terrorist Financing**. You must report your concerns to the **Ethics & Compliance Office** and Legal Department as soon as possible."*

3.2 "A **Business Partner** wants to pay an invoice for a large sum in cash. What should I do?"

*"Cash payments are often used for **Money Laundering**. You should contact the **Ethics & Compliance Office** as soon as possible."*

3.3 "I know that a **Business Partner** is being investigated as they are suspected of **Money Laundering**. Can I tell them?"

"No, you must not tell them. Telling them would tip them off concerning the investigation. This would be in breach of this Policy and will be against the law in most cases."

3.4 "A **Business Partner** has told me that they give money to a charity that I have read in a reputable newspaper is linked to the funding of terrorism. What should I do?"

*"It is possible that your **Business Partner** is funding terrorism (perhaps inadvertently). You must report your concerns to the **Ethics & Compliance Office** and the Legal Department."*

SANCTIONS AND TRADE CONTROLS POLICY

1. POLICY SUMMARY

Summary

Applicability

What You Must Do

Questions and Reporting Breaches

1. Policy Summary

1.1 Summary

(a) We conduct business globally and comply with **Trade Controls** and **Sanctions** laws, rules, and regulations. We identify, manage, and minimize risks and prevent breaches.

(b) **Trade Controls** and **Sanctions** limit trade or the provision of money, goods or services to certain countries, organizations, companies, and people. Sometimes, it is possible to obtain a **License** from a Government or regulator that will allow you to conduct business that would otherwise be illegal.

(c) Many countries impose **Trade Controls** on the import, export, transfer, re-export and re-transfer of military goods, sensitive or proprietary technology information and goods, and **Dual-Use Items**. The rules are complex and can capture the transfer of software and data, as well as the movement of equipment and physical goods.

(d) **Sanctions** can also restrict the trade in goods and the provision of money, goods or services to **Sanctioned Persons** and **Sanctioned Countries**.

(e) Both **Sanctions** and **Trade Controls** often apply extra-territorially (outside of the borders of the regulating country).

(f) This Policy sets out certain requirements and guidance to prevent any breaches of **Trade Controls** and **Sanctions**.

(g) If you have any doubts, questions or concerns about this Policy, you should contact the **Ethics & Compliance Office** on the Helpline (**helpline.taqa.com**).

(h) You must:

(i) Ensure that **Business Partners** are subject to **Sanctions Screening** before any contracts are signed or any agreements are entered into or renewed. Please refer to the **Business Partner Due Diligence Policy** for more details on the screening process;

(ii) Obtain prior written approval of the Legal Department and the **Ethics & Compliance Office** before having any dealings involving a **Sanctioned Person** or **Sanctioned Country**;

(iii) Undertake a geographic risk-assessment before any import, export, transfer, re-export, or retransfer of any **Items** takes place;

(iv) Ensure that nothing is exported, transferred, re-exported, or re-transferred to a **Sanctioned Country** without the prior written approval of the Legal Department and the **Ethics & Compliance Office**;

(v) Understand the **Trade Controls** relevant to any **Items** that you deal with as part of your role;

(vi) Obtain prior written approval from the Legal Department and the **Ethics & Compliance Office** before any export, transfer, re-export, or re-transfer of **Controlled Items**;

(vii) Obtain advice from the Legal Department and the **Ethics & Compliance Office** prior to entering into any communications with a Government or regulator regarding **Sanctions** and **Trade Controls**;

(viii) Comply with the laws of your country or countries of citizenship. It is your responsibility to understand any relevant requirements; and

(ix) Follow this Policy and any policies imposed by the **Business** you work for.

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability and reputational damage. You may also be subject to disciplinary action, including but not limited to, termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the Legal Department and the **Ethics & Compliance Office** for approval.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** in which you work.

(b) Report known or suspected violations of this Policy as soon as possible.

(c) Complete any training and required declarations associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

2. POLICY REQUIREMENTS

- Sanctions
- Trade Controls
- Recordkeeping
- Contractual Protections
- Communications with Governments and Regulators

2. Policy Requirements

2.1 Sanctions

TAQA Group does not do business with **Sanctioned Persons** or **Sanctioned Countries**. Trading with such **Sanctioned Persons** or **Sanctioned Countries** is illegal, and it carries a risk that could result in criminal penalties.

There are many different types of **Sanctions**, including:

(a) Targeted financial restrictions on people, companies, governments, and countries, such as asset freezes or "blocking" sanctions;

(b) Economic sanctions that restrict the financing or provision of financial services in relation to certain goods, services, or financial products;

(c) Trade-related restrictions that stop or limit the provision of certain goods and services in relation to targeted people, companies, governments, and countries;

(d) Travel bans on named individuals; and

(e) Anti-boycott regimes.

Sanctions can target either specific individuals, entities, industry sectors or entire countries and territories. **Sanctioned Persons** can be anywhere in the world, and individuals are added to the lists of **Sanctioned Persons** everyday. It is therefore important that you regularly check the status of all **Business Partners** which can be achieved most efficiently by the use of automated screening tools. If you are unsure about checking the status of **Business Partners**, then please contact the **Ethics & Compliance Office**.

You must always:

(a) Ensure that **Business Partners** are subject to **Sanctions Screening** before any contracts are signed or any agreements are entered into or renewed. Anyone who is a **Sanctioned Person** or linked to a **Sanctioned Country** will need very careful assessment before any business is conducted. Please refer to the **Business Partner Due Diligence Policy** for more details on the **Sanctions Screening** process;

(b) In accordance with the **Business Partner Due Diligence Policy**, obtain prior written approval of the Legal Department and the **Ethics & Compliance Office** before considering having any dealings involving a **Sanctioned Country**, **Sanctioned Person,** or any person linked to a **Sanctioned Country**;

(c) Undertake a geographic risk-assessment before the import, export, transfer, re-export, or retransfer of any **Items** takes place;

(d) Ensure that nothing is exported, transferred, re-exported, or re-transferred to a **Sanctioned Country** without the prior written approval of the Legal Department and the **Ethics & Compliance Office**; and

(e) Comply with the laws of your country or countries of citizenship. It is your responsibility to understand any relevant requirements imposed by your country or countries of citizenship as they may restrict you from being involved in certain activities.

Businesses must also consider the **Sanctions**-related terms of **TAQA's** agreements prior to entering into any contracts with **Business Partners**. If a **Business** requires any guidance, they should contact the Legal Department and the **Ethics & Compliance Office**.

You may be in breach of **Sanctions**, in the following red flag situations:

Examples of Red Flags

- You deal with a supplier that is owned by a person from a **Sanctioned Country**.
- You buy, sell, or transport goods coming from or going to a country, group, or individual targeted by **Sanctions**.
- Your supplier may be targeted by **Sanctions** or may be located in a jurisdiction where many people targeted by **Sanctions** are located, or may be associated with someone targeted by **Sanctions**.
- Your contractor is owned by a **Politically Exposed Person**.
- Your distributor deals in certain high-risk products (e.g. advanced computers or **Dual-Use Items** or military technology).

Further details on how red flags are addressed in the context of our **Due Diligence** on our **Business Partners** can be found in the **Business Partner Due Diligence Policy**.

2.2 Trade Controls

Many countries impose **Trade Controls** on the export, import, transfer, re-export, and re-transfer of military goods and **Dual-Use Items**.

Broadly, **Dual-Use Items** are items that are capable of a military or civilian use. The rules are complex and can capture the transfer of **Technical Data**, as well as the movement of physical items. Often the controls are related to the identity of the country of destination, the exporter, or the recipient of the **Items** and can extend to **Dual-Use Items**.

Each Business must ensure that it:

(a) Understands the **Trade Controls** relevant to and classification of any **Items** that it exports, imports, transfers, re-exports, and re-transfers;

(b) Appropriately secures and maintains any **Controlled Items** in accordance with applicable laws and regulations, including, where necessary, preventing **TAQA Personnel** of certain citizenships and nationalities from accessing the **Controlled Items**;

(c) Implements any necessary travel protocols and data security measures needed to protect **Technical Data** relating to **Controlled Items**;

(d) Secures where required end-user certificates and includes an appropriate statement on relevant sale, supply, and shipping documents preventing the diversion of the **Items**; and

(e) Complies with the terms of any **Licenses**.

You must ensure that you:

(a) Understand the **Trade Controls** relevant to any **Items** that you deal with as part of your role; and

(b) Obtain prior written approval from the Legal Department and the **Ethics & Compliance Office** before any export, transfer, re-export, or re-transfer of **Controlled Items**.

Examples of Red Flags

- The goods you are shipping appear to have (or actually have) both a civilian and a military use.
- The technology you are transferring appears to have (or actually has) a military use.
- Your customer is reluctant to confirm routine commercial matters, such as the end-user of the goods.
- The person paying for your equipment has a different name or location than the recipient of the goods.
- Your goods are subject to an unusual shipping or packing request, such as an abnormal shipping route.
- Your goods are being used by the military or a government in a destination which could be considered high risk.
- Your goods are of high value and are being paid for in cash.

2.3 Recordkeeping

Trade Controls often create specific recordkeeping and reporting requirements. Many countries also have specific documentary requirements, such as a requirement to use state specific **License** language on shipping documents, recording and reporting the use of **Licenses** and specified retention periods for records.

Each **Business** must adopt procedures to manage recordkeeping and reporting requirements, taking into account the specific requirements of **Licenses** provisions and regulatory requirements applicable to the conduct of their **Business**.

2.4 Contractual Protections

When entering into contracts with **Business Partners**, you should consider the inclusion of contractual protections that ensure that they and their **Directors**, officers, employees, agents, and representatives:

(a) Are not in violation of, and have never violated, any applicable **Sanctions**;

(b) Are not, and have never been, a **Sanctioned Person**;

(c) Are not engaged in any transactions or conduct that is likely to result in them or any other person becoming a **Sanctioned Person**;

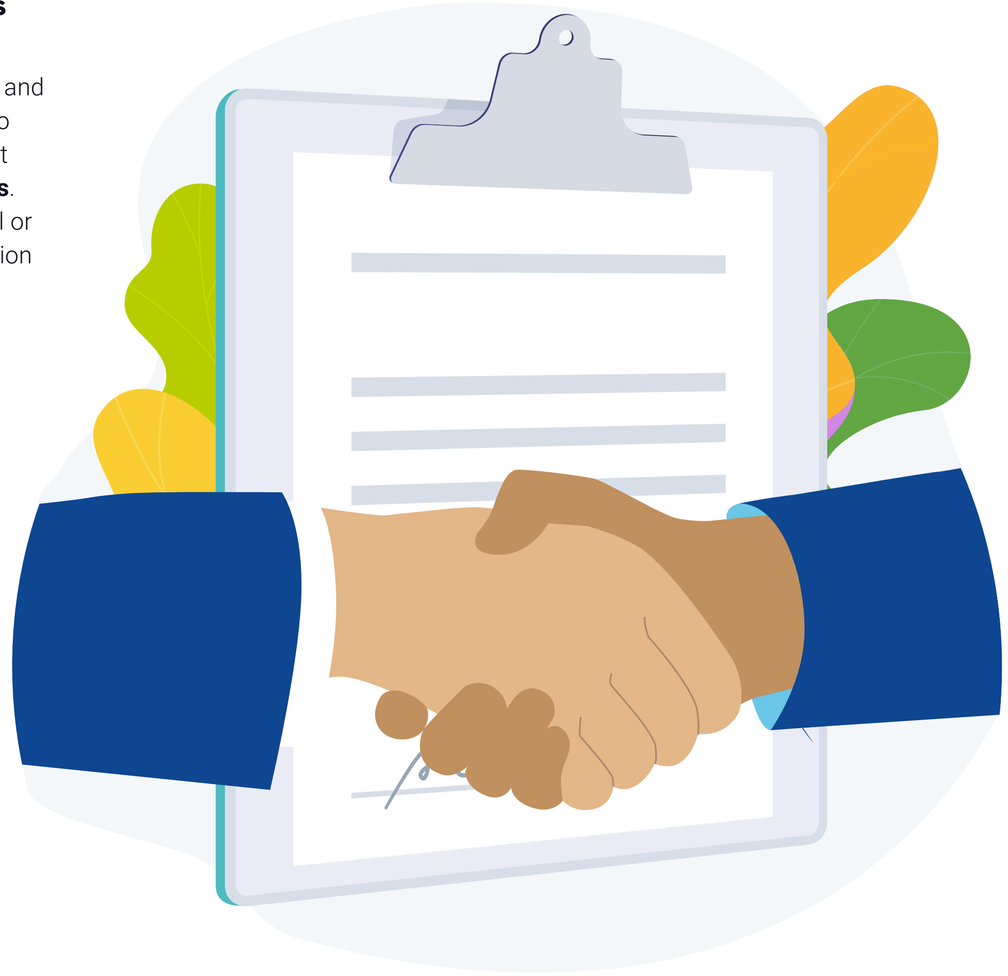
(d) Have not conducted and are not conducting any business dealings or activities with or for the benefit of, or are otherwise involved in any business in or with, any **Sanctioned Country** or with any **Sanctioned Person**; and

(e) Are not causing, and have not caused, any other person to be in violation of any **Sanctions**.

These contractual protections are not a substitute for conducting **Sanctions Screening** in accordance with the **Business Partner Due Diligence Policy**.

2.5 Communications with Governments and Regulators

You must obtain advice from the **Legal Department** and the **Ethics & Compliance Office** prior to entering into any non-routine communications with a Government or regulator regarding **Sanctions** and **Trade Controls**. Non-routine communications could involve potential or actual breaches of law, disclosures, audits, information requests, or the start of an investigation.



3. FREQUENTLY ASKED QUESTIONS

3. Frequently Asked Questions

3.1 "Can you give me an example of a **Sanctions** restriction that might be relevant to the **TAQA Group**?"

TAQA *could be violating* ***Sanctions*** *if it imports certain goods into certain countries. Those goods include but are not limited to certain pipes, tubes, casings, drills, rock-drilling or earth boring tools, vessels, and floating cranes.* ***TAQA*** *could also violate* ***Sanctions*** *if it pays or provides goods or services to certain* ***Sanctioned Persons*** *which include a number of large companies around the world.*

3.2 "Do I need to worry if I am doing business with a company that is ultimately owned by a national of a **Sanctioned Country**?"

Yes, in these circumstances you must stop doing business with the company immediately and notify the Legal Department and the ***Ethics & Compliance Office.*** *You may resume business once the company has undergone* ***Sanctions Screening*** *and only if you have received written approval from the Legal Department and the* ***Ethics & Compliance Office****. Please refer to the* ***Business Partner Due Diligence Policy*** *for more details on the screening process.*

3.3 **"**Can you please give me some examples of what items are **Dual-Use Items**?"

*Many items are specifically controlled on the basis that they are **Dual-Use Items**. They include certain:*

(a) Deep-hole drilling machines and drill bits;

(b) Space qualified solar cells, cell-interconnect-cover glass assemblies, solar panels, and solar arrays;

(c) Certain rotors and stators;

(d) Certain types of piping;

(e) Certain pumps and valves;

(f) Vibration testing equipment;

(g) Certain chemicals and microorganisms; and

(h) Software and technology related to any of the above.

However, it is important to note that almost anything can be dual-use as most items can have both commercial and military applications, so you need to consider where your items are going and who will ultimately be using them.

3.4 "What about US-origin goods – are there any restrictions I need to be aware of?"

Yes, US export control rules restrict the exportation, re-exportation, and transfer of (1) US-origin goods, and (2) certain non-US origin goods that include US-origin components or technology. However, not all items that are subject to US export control rules are necessarily prohibited for exportation, re-export, or transfer. Accordingly, whether a US-origin good – or non-US-origin good that incorporates US-origin components/technology – is permitted for exportation, re-exportation, or transfer is dependent on the facts.

*If you are in any doubt about these issues, please seek guidance from the Legal Department and the **Ethics & Compliance Office***

4. PRE-APPROVALS PROCESS

4. Pre-Approvals Process

You must seek pre-approvals from the Legal Department and the **Ethics & Compliance Office** or, where applicable, via the local representatives of the Legal Department and the **Ethics & Compliance Office** within your **Business**, as required by this Policy. You must also follow the process set out in the **Business Partner Due Diligence Policy** before doing business with a **Sanctioned Country, Sanctioned Person,** or any person linked to a **Sanctioned Country**:

(a) Follow any additional internal approval processes before seeking pre-approval from the Legal Department and the **Ethics & Compliance Office**;

(b) Follow the instructions and complete the appropriate pre-approval online form which is available on the Helpline (**helpline.taqa.com**); and

(c) Submit the completed online form to the **Ethics & Compliance Office** using the Helpline (**helpline.taqa.com**).

ANTITRUST POLICY

1. POLICY SUMMARY

- Summary
- Applicability
- What You Must Do
- Questions and Reporting Breaches

1. Policy Summary

1.1 Summary

(a) **Antitrust Laws** exist in numerous jurisdictions globally, and are designed to promote fair competition and prevent anti-competitive behaviour. We conduct ourselves in a manner that is compliant with **Antitrust Laws** applicable to our **Businesses** in the local and international markets where we have a presence. It is important that all **TAQA Group Personnel** are aware of and comply with the **Antitrust Laws** that are relevant in the context of **TAQA Group's** activities.

(b) We are subject to **Antitrust Laws** wherever we operate (unless we have an exemption). Consequences of breaching these laws can be serious for both **TAQA Group** and for individual employees who may face criminal prosecution regardless of where they are geographically located.

(c) Anti-competitive behavior can take multiple forms, including:

(i) Entering into **Anti-Competitive Agreements** with **Competitors** and, in some circumstances, **Distributors**, **Suppliers** and/or **Customers**; and

(ii) Abuse of a dominant market position by **TAQA Group**.

(d) When we engage in mergers & acquisitions, we may also be subject to the merger control laws of many jurisdictions, including jurisdictions where either **TAQA Group** or the relevant counterparty may not be active.

(e) Contact the Legal Department and the **Ethics & Compliance Office** immediately if you have concerns that **Antitrust Laws** may have been breached.

(f) This Policy sets out the key principles that are followed in the majority of countries that adopt antitrust best practice. In particular, it covers the prohibition of **Anti-Competitive Agreements** and abuse of a dominant market position, as well as practical tips to be followed when conducting mergers & acquisitions, handling investigations and managing documents.

(g) This Policy is intended to provide awareness regarding antitrust rules to enable recognition of antitrust issues and when to seek guidance.

(h) In short, you must:

(i) Be aware of the existence of **Antitrust Laws** in all dealings with **Competitors;**

(ii) Ensure that **TAQA Group** acts independently on the market and does not coordinate its market conduct with **Competitors.**

(iii) Not agree or communicate with **Competitors** on: prices or related topics (such as discounts, timing of price changes, margins or overheads), bids, sales, market shares, customers, trading conditions, allocation of customers or regions, capacity, supply terms or output, product cost information, strategic or marketing plans, R&D plans, boycotting of competitors, suppliers or customers;

(iv) Not share **Commercially Sensitive Information** with **Competitors**. If you receive such information from or about a **Competitor**, you must report it to the Legal Department and the **Ethics & Compliance Office** immediately;

(v) Contact the Legal Department and the **Ethics & Compliance Office** before entering into any collaborative agreements with **Competitors** (e.g. joint ventures, research and development agreements, licensing agreements, or merging with or acquiring **Businesses**);

(vi) Approach agreements with **Customers** or **Distributors** with caution, and ensure that all agreements are property reviewed and approved by the Legal Department. If you are aware, or become aware, of any possible **Antitrust** issues, immediately report these to the Legal Department and the **Ethics & Compliance Office**;

(vii) Contact the Legal Department before: restricting **Distributors** from selling to particular customers or territories; refusing to deal with **Customers** / **Distributors**; entering into exclusive agreements or sending price announcements to customers, and notify the **Ethics & Compliance Office** of any issue or matter that you have had to raise with the Legal Department;

(viii) Be aware that where **TAQA Group** has a high market share for any product in any jurisdiction, more care is required in commercial dealings, as certain of our activities may be seen as the abuse of a dominant market position and may be unlawful; and

(ix) If you have any doubts, questions or concerns about this Policy you should contact the **Ethics & Compliance Office** on the Helpline (**helpline.taqa.com**).

1.2 Applicability

(a) This Policy applies to **TAQA Group** and to **TAQA Group Personnel**.

(b) Failure to follow this Policy puts yourself, your colleagues, and **TAQA Group** at risk of civil and/or criminal liability, and reputational damage. You may also be subject to disciplinary action, including but not limited to termination of your employment.

(c) **Businesses** may establish standards that are stricter than this Policy. Any other exceptions to or deviations from this Policy must be submitted to the **Ethics & Compliance Office** for approval.

1.3 What You Must Do

(a) Understand and comply with the requirements of this Policy, the **Code of Ethics & Business Conduct**, and any standards introduced by the **Business** that you work for.

(b) Report known or suspected violations of this Policy as soon as possible to the **Ethics & Compliance Office**.

(c) Complete any training associated with this Policy.

(d) Understand and comply with the requirements of any applicable laws and regulations, and where this Policy sets a conflicting or lower standard than relevant laws or regulations you must comply with such laws or regulations rather than with this Policy.

1.4 Questions and Reporting Breaches

(a) Direct any questions, concerns, or any known or suspected violations of this Policy to the **Ethics & Compliance Office** in person or through the Helpline (**helpline.taqa.com**).

(b) We have a zero-tolerance approach to retaliation against anyone raising a concern. Those who engage in retaliatory behavior will be subject to disciplinary action.

2. ANTI-COMPETITIVE AGREEMENTS

- Possible Exemptions
- Types of Anti-Competitive Agreements
- Take Care in all Dealings with Competitors
- Dealings with Customers / Distributors / Suppliers Can Raise Issues

2. Anti-Competitive Agreements

2.1 Antitrust Laws

(a) **Antitrust Laws** prohibit **Anti-Competitive Agreements**. It does not matter how these agreements are structured or what they are called. **Antitrust Laws** also cover agreements or "understandings" that are not in writing and which have not been formalized or implemented.

(b) Agreements between **Competitors** acting at the same level of the supply chain (horizontal agreements) are most likely to give rise to antitrust issues. However, agreements between companies operating at different levels of the supply chain (vertical agreements), such as a manufacturer and **Distributor** may also be problematic in certain circumstances. Therefore, as mentioned above, it is important to ensure that all agreements are property reviewed and approved by the Legal Department before they become legally binding.

2.2 Possible Exemptions

There may be exemptions from **Antitrust Laws** for agreements that result in benefits that are passed onto consumers and are in fact pro-competitive overall. **TAQA Group** activities related to the production, distribution, and transport of electricity and water are exempted from application of the **UAE Competition Law** by the **UAE Competition Authority**.

It is very difficult to avail exemptions to **Antitrust Laws**, especially for horizontal agreements. An assessment of whether an agreement is pro-competitive or falls under an exemption is complex and you should never self-assess. Consult both the Legal Department and the **Ethics & Compliance Office** for antitrust assessments.

2.3 Types of Anti-Competitive Agreements

The below table sets out different types of **Anti-Competitive Agreements**.

Type of Competitive Agreement	Description
Price Fixing	Fixing purchase or selling prices (or agreeing discounts), or fixing other key commercial terms between **Competitors** regardless of whether the prices are fixed at a minimum, maximum or within a particular range
Output Restrictions	Agreeing to stop or reduce production or supply to influence market conditions, including restricting exports within the EU Internal Energy Market
Market Sharing	Dividing up (or 'sharing') markets between **Competitors** by, for example, territory, product, **Customer** group, or **Customer**
Collective Boycott	Agreeing to boycott collectively other **Competitors**, **Suppliers** or **Customers**
Bid Rigging	Agreeing not to bid against **Competitors**, or to bid at a certain price, or otherwise allocating bids
Resale Price Maintenance	Setting the price at which **Customers** or **Distributors** must onsell products (this includes setting a minimum price), or otherwise encouraging them to stick to a certain price or price level (such as by fixing margins; making the grant of rebates or reimbursement of promotional costs subject to a given price level; warnings and similar practices inducing price maintenance)
Exclusivity	Granting **Distributors** an exclusive territory, an exclusive customer group or the exclusive right to market a product may in some circumstances be illegal
Information Exchange	Sharing **Commercially Sensitive Information** with **Competitors**

2.4 Take Care in all Dealings with Competitors

(a) You need to be aware of the need to comply with **Antitrust Laws** in all dealings with **Competitors.** You must be cautious when in contact with our **Competitors** and consider whether you should even be in contact with such a **Competitor**.

(c) We often deal with companies who are at times **Competitors** and at other times are **Suppliers** or **Distributors**. It may not always be clear whether a company is a **Customer / Supplier / Distributor** or a **Competitor** in every context. If you have any questions about this, contact the Legal Department and the **Ethics & Compliance Office.**

DO NOT		
Discuss or Agree with Competitors	• Prices or related topics (such as discounts, timing of price changes, margins or overheads) • Bids, sales, market shares or customers • Sharing of customers or regions • Capacity, supply terms or output	• Product cost information • Strategic or marketing plans • R&D plans • The boycotting of **Competitors**, **Suppliers**, or **Customers**
Exchange Commercially Sensitive Information with Competitors such as at Trade Association Meetings, Standard Setting Meetings, or Informal Gatherings	**Antitrust Laws** prohibit exchanges of information which take place between multiple competitors (such as at a trade association meeting). While it is fine for such meetings to be used to discuss general issues, (health and safety, environmental issues, tax, etc.), they should never be used to discuss or agree an "industry solution" to a competitively sensitive commercial issue or to exchange **Commercially Sensitive Information**. All trade association meetings should proceed on the basis of a clear agenda, and an explicit statement that the meeting shall not discuss any anti-competitive issues. If the discussions at a trade association meeting or any other meeting with **Competitors** turn to a prohibited topic, make sure you object and insist that your objection is recorded in the minutes and inform the **Ethics & Compliance Office** immediately. If the discussion continues, leave the meeting and immediately report the matter to the **Ethics & Compliance Office**.	
Receive or Exchange Commercially Sensitive Information directly from/ with Competitors	This includes **Commercially Sensitive Information** on a **Competitor** shared by only one company or person. You should not exchange or request such information. If you receive such information from a **Competitor** without requesting it, if you do not respond with a clear statement that you do not want to receive it, you might breach **Antitrust Laws**. Failing to respond is not an appropriate response. If you receive such information, contact the **Ethics & Compliance Office** immediately. Please note that the rules on exchanging **Commercially Sensitive Information** also apply in the context of joint ventures with **Competitors**. Generally, joint venture parties can exchange information necessary for planning for post-closing and operation of the planned joint venture, including information about the costs incurred in connection with the planning and development of the joint venture. It may be permissible to share such sensitive information that otherwise should not be disclosed, but only if the following procedures are followed: • The information shared must only be shared on a need-to-know basis, i.e., the information shared must be limited to only what is necessary for joint venture planning and closing of the transaction and must be shared only between individuals who need to exchange that information for the joint venture planning. • The information must not be used for any other purposes or in any way that affects competition between the companies (e.g., pre-closing sales, pricing, marketing).	
Enter Collaborative Agreements with Competitors without First Consulting the Ethics & Compliance Office and Legal Department	This includes joint ventures, jointly operated assets, research and development arrangements and other cooperation agreements. The **Antitrust Laws** require that joint venture parties continue to operate as two, separate, independently run companies both during the joint venture planning and after the planned joint venture is formed. The joint venture parties should not take any action that appears to be an attempt to reduce competition between them.	

2.5 Dealings with Customers / Distributors / Suppliers Can Raise Issues

(a) Agreements with **Customers** / **Distributors** / **Suppliers** are less likely to be **Anti-Competitive Agreements**. Even so, certain restrictions are illegal and you need to approach negotiations for agreements with **Customers** / **Distributors** / **Suppliers** carefully. If you have any questions about this, contact the **Ethics & Compliance Office.**

DO NOT	
Control the Price at which Customers/ Distributors Resell	This could be by fixing the price or imposing a minimum resale price. **Customers** / **Distributors** should be free to determine their own resale price. Setting a maximum or recommended resale price will not usually raise antitrust issues as long as it is not combined with terms or conditions that are in fact incentives to stick with the recommendation (e.g. bonuses or rebates for applying a recommended price). Check with the Legal Department and the **Ethics & Compliance Office** if you require assistance with any of the above. You should also seek guidance if you propose to include any restrictions on the territories to which **Distributors** can sell **TAQA Group's** products.
Do Business with any third party without following the requirements of the Business Partner Due Diligence Policy, the Sanctions and Trade Controls Policy, and ensure that you consider Antitrust Laws	There must be a valid reason for taking this action, which should be clearly recorded.
Enter Exclusive Arrangements with Customers without checking with the Legal Department and the Ethics & Compliance Office	This includes agreements that the **Customer** will purchase all or substantially all of its requirements for a particular product or service from the company. Long-term arrangements are more likely to be problematic, but what amounts to "long-term" in this context will vary from case to case. Also, check with the Legal Department and the **Ethics & Compliance Office** before entering into an agreement with a **Customer** where the sale of one product or service is connected with the **Customer** purchasing another product or service.
Share Commercially Sensitive Information provided by one Customer to another Customer	Otherwise, we could be found to be an intermediary for information sharing between competing **Customers** and could be in breach of **Antitrust** and **Data Protection Laws**.
Send price announcements to Customers before checking with the Legal Department and the Ethics & Compliance Office	Under certain circumstances, signalling price changes in advance of the effective date could be illegal. It may be more appropriate to send announcements that are specific to the individual **Customer**.

3. ABUSE OF DOMINANT MARKET POSITION

- Antitrust Laws Prohibit the Abuse of a Dominant Market Position
- Examples of Potentially Illegal Conduct

3. Abuse of Dominant Market Position

3.1 Antitrust Laws Prohibit the Abuse of a Dominant Market Position

Antitrust Laws prohibit the abuse of a dominant market position such as unlawfully exercising market power or abusing your position as a **Monopoly**.

(a) Holding a dominant market position is not a breach of **Antitrust Laws,** the abuse of a dominant market position is. Some legitimate business practices become prohibited once a dominant market position is established.

(b) "Dominance" is generally viewed as the ability of a company to act independently of its competitors, customers, and consumers. Market share is a key factor in determining whether a company is dominant in a particular market.

(c) In areas where we have high market shares (e.g. above 40%), the best approach is to assume a dominant market position and ensure that our conduct in the market is not abusive.

(d) While we may be subject to oversight from non-competition regulators in certain jurisdictions, compliance with sector-specific regulations (including price regulation) is not typically a defense to anti-competitive conduct in most jurisdictions (e.g. in Europe). In those jurisdictions, **Antitrust Laws** continue to apply even where prices and other conduct are regulated.

3.2 Examples of Potentially Illegal Conduct

The below table sets out examples of potentially illegal conduct.

Refusal to Supply	Refusing to sell to new **Customers** or stopping sales to existing **Customers** without valid reason
Predatory Pricing	Setting below market prices with the intention of driving a **Competitor** out of the market or preventing the entry of a **Competitor** into the market
Loyalty Rebates and Discounts	Where the **Customer** receives an incentive to purchase exclusively from a particular **Supplier**. However, quantity rebates or discounts that are related to cost savings, and which are applied to all **Customers**, would not be problematic
Discrimination	Charging different prices or imposing different trading terms, for **Customers** who are broadly in the same position, and where the differences cannot be justified
Excessive Pricing	Over-charging **Customers** a price so high that has no connection to the value of the goods or services being sold
Tying and Bundling	Making the sale of one product conditional on the **Customer** purchasing another

Always consult the Legal Department and the **Ethics & Compliance Office** before engaging in any of the types of actions mentioned above or taking any unusual pricing decisions.

4. MERGERS & ACQUISITIONS

4. Mergers & Acquisitions

4.1 Certain transactions, not just acquisitions, may be subject to merger control laws including outside the jurisdiction in which the transaction takes place. If you are involved in any mergers and acquisitions on behalf of **TAQA Group** you must ensure that you are aware:

(a) Of the merger control laws in relevant jurisdictions where you seek to undertake mergers and acquisitions. It is important to remember that just because **TAQA Group** does not have operations in a certain jurisdiction this does not automatically mean that the merger control laws of third countries are not applicable.

(b) That most jurisdictions with merger control laws or rules operate a pre-approval regime, which means that a transaction must be notified to the relevant authority before the transaction has completed. Failure to report to the relevant authority can lead to significant fines and the potential reversal of the transaction.

(c) That merger control authorities review transactions to assess their effects on competition and may, in certain circumstances, ban or impose strict conditions on intended mergers & acquisitions.

(d) That a merger is not always obvious. In some jurisdictions, it is based on the acquisition of a certain equity percentage (e.g. the acquisition of a 50% stake) and is therefore relatively easy to apply. However, in other jurisdictions, you will need to assess whether you are acquiring 'control' of a market. In certain circumstances, the acquisition of assets (including financial assets), minority stakes or the creation of a joint venture may also require notification to merger control authorities.

(e) When considering potential mergers & acquisitions, you should contact the Legal Department to assess whether or not merger control needs to be taken into account and notify the **Ethics & Compliance Office** of the possible mergers & acquisitions activity.

4.2 Further, during due diligence for potential mergers & acquisitions (and in the period between signing and completion), it is possible that **TAQA Group** will need to access confidential non-public information about potential targets or partners. **Antitrust Laws** still apply in such circumstances and the **Ethics & Compliance Office** will assist in ensuring that appropriate procedures are in place for the potential exchange of such information.

5. GENERAL DOCUMENT MANAGEMENT

5. General Document Management

6.1 When creating documents you should consider that they might be read by antitrust authorities or **Third Parties.**

(a) This applies to all written documents, including emails and handwritten notes. Also consider how documents can affect the strategy for mergers and acquisitions. Where merger notifications are required as part of an acquisition (see section 4 above), many merger control authorities will issue detailed requests for internal documents of the parties (e.g. board papers, management presentations, analyses of the deal and/or the market), in order to understand the purpose of the transaction and how the parties view competition in the market.

PRACTICAL TIPS WHEN CREATING DOCUMENTS		
Avoid Using the Following Terms (or similar) *This list is not intended to be exhaustive*	• Dominant/dominate the market or the competition • Attack • Kill off the competition • Squash the threat • Drive out of the market • Lock-out competitors • Divide/share the market • Tie-in/tie-down	• Increase/fix prices • Control prices • Market power • Eliminate competition • Prevent imports • Obstruct exports • Boycott • Burn/destroy this document / delete this e-mail after reading
Avoid Language Which Could Have Alternative Meanings	Be clear about what you are saying. Give as much background or context as possible and make sure any analysis is supported by evidence. Do not exaggerate the position or give misleading impressions.	
Be Extremely Cautious About Presenting Detailed Market Shares	Either for **TAQA Group** or its **Competitors**. This could be problematic, particularly where the information has been gathered in the context of a prospective acquisition.	
Keep a Clear Note of the Source	Where presenting external information clearly mark the source, e.g. legitimate competitive intelligence from a **Customer** or information obtained from a market research provider or a pricing benchmark in order to be able to demonstrate that the information was obtained in an appropriate manner. Identify any information which is an estimate.	

(b) If you receive an inappropriate communication, email or a document from a Competitor which you feel breaches Antitrust Laws:

(i) Immediately notify the Legal Department and the **Ethics & Compliance Office**;

(ii) Do not review the email/document further;

(iii) Do not use or circulate the information to other people you work with; and

(iv) Reply with a clear statement that you do not wish to receive this type of information.

6. FREQUENTLY ASKED QUESTIONS

6. Frequently Asked Questions

6.1 "I am the account manager for our biggest customer. From time to time, I receive detailed information from their purchasing director about the prices our competitors are charging. I have shared this with my colleagues. Does this infringe **Antitrust Laws**?"

Receiving information from Customers about what prices Competitors are offering is a normal part of the commercial negotiation process.

*However, if a **Competitor** was disclosing the information to our **Customer** with the intention that our **Customer** would pass this on to you, this could be an illegal exchange of **Commercially Sensitive Information** between **Competitors**. If you think that might be happening, contact the Legal Department and the **Ethics & Compliance Office** who will provide further guidance.*

*Moreover, you should not request competitor prices or price-related information from any **Customer**.*

*If you share **Competitor** prices that you have received with colleagues, you should include the source of this information.*

6.2 "I attended a trade conference to discuss international trends in the Oil & Gas sector. A representative from a competitor, Company B, was discussing new climate change legislation and that Company B plans to pass on 100% of a new carbon tax directly to its customers. I am aware that my company is also planning to implement certain changes to pricing to reflect the new carbon tax, but I did not mention this to the representative from Company B. I did, however, take the information back to my line manager to consider whether we should be following a similar policy. However, after discussion, we decided to follow our existing strategy."

*It is legitimate to attend meetings of trade and industry bodies as a representative of **TAQA Group** to discuss generic issues, e.g. health and safety, environmental issues or tax. However, at such meetings representatives should not discuss industry solutions to external factors or their own planned strategic responses, in relation to competitively sensitive areas such as dealings with customers generally, and in particular as regards price, sales volumes, dealings with specific customers or specific suppliers, production input price or volume or output volumes, etc.*

*The prohibition on exchanging **Commercially Sensitive Information** does not just apply to the person sharing the information, but also any person who receives that information.*

*It is not relevant that the exchange was only a one-off and it is not relevant that **TAQA Group** did not act on the information by changing its own plans.*

*Both you and **TAQA Group** could both be liable for having infringed **Antitrust Laws** in this situation.*

*In such circumstances, you should have intervened to tell the representative from Company B that the discussion was inappropriate and left the meeting or the conversation. You should have asked that your objection was registered in the meeting minutes and that it was recorded that you left the meeting. Following the conversation, you should have contacted the Legal Department and the **Ethics & Compliance Office** immediately to report the content of the meeting.*

6.3 "I am engaged in a tender process and have been contacted by my **Competitor**, Company B, who is also planning to bid. Company B has asked me to bid above a certain level, saying that in return, it will bid above our price for the next one. Is this ok?"

*No. This gives rise to serious issues. Agreeing or discussing with a **Competitor** how you will bid on a particular tender, amounts to bid-rigging and is a breach of **Antitrust Laws**. Public tender procedures in particular are closely monitored by many antitrust authorities, including by the use of algorithms and artificial intelligence (AI).*

6.4 "A new competitor has just entered into the market and is gaining some of our market share. We think its current pricing strategy is unsustainable and if we react by aggressively lowering our own prices (possibly below cost) then we can regain our lost revenues and the new competitor may need to consider exiting the market."

Although we try to compete actively in all markets, and generally have freedom to autonomously set prices, *where we have a strong market position you need to exercise particular caution. If we are found to have a dominant position in the market, the setting of prices below cost with the intention of driving a* ***Competitor*** *out of the market may breach* ***Antitrust Laws****. You should seek guidance from the Legal Department and the* ***Ethics & Compliance Office****.*

6.5 "We are considering acquiring several production assets from a company to assist with our growth plans. Do I need to consider whether merger control clearances might be required?"

"Yes. Merger control laws apply regardless of whether you are acquiring assets (whether tangible or otherwise) or shares in another company. You should check with the ***Ethics & Compliance Office*** *whether you need to include provision for merger control in the transaction documents and consider timing implications of any potential approval processes."*

6.6 "We are planning to acquire a minority stake in a company which is active in a product market which is completely unrelated to the activities of **TAQA Group**. Do I still need to consider merger control laws even though this stake will not allow **TAQA Group** to control the target company and there are evidently no concerns that **TAQA Group** will be increasing its market share in any of the areas where it is active?"

Yes. Merger control laws may apply even for the acquisition of a minority stake. For the purposes of establishing whether a merger control filing is required, in certain jurisdictions it may be irrelevant that ***TAQA Group*** *does not currently compete with the target company or even that the deal does not seem to involve that jurisdiction. You should check with the* ***Ethics & Compliance Office*** *whether you need to include provision for merger control in the transaction documents.*

GLOSSARY

Contacts

Definitions

Revision History

Contacts

You can ask questions or raise concerns to the Ethics & Compliance Office via the Helpline (**helpline.taqa.com**), which is provided by an independent service provider, and allows you the option to remain anonymous. For further details please see the **Speaking Up Policy**.

Definitions

ADX

The Abu Dhabi Securities Exchange.

Anti-Competitive Agreement(s)

Agreements or concerted practices which are intended to, or that have the effect of, preventing, restricting, or distorting competition. This can include written and oral agreements; agreements that are not legally binding or that never actually happen; informal arrangements and understandings; decisions by trade associations; and exchanges of **Commercially Sensitive Information**.

Anti-Money Laundering (or AML)

Laws or regulations designed to stop the practice of Money Laundering.

Antitrust Laws

A body of applicable laws, regulations, rules, orders and other obligations that regulate competition in markets.

Blackout Period

A period prescribed by **TAQA Group** (other than a **Closed Period**) during which TAQA Group Personnel are prohibited from **Trading** in **TAQA Group Securities**.

Books and Records

Includes accounts, invoices, correspondence, papers, and other documents that record and reflect the **TAQA Group's** business, transactions, and other activities whether in written or in any other form (including electronic).

Bribery (Bribe)

Any gift, payment, offer, promise to pay, or authorization for anything of value provided, directly or indirectly, to or for the use or benefit of any person for the purpose of influencing any act, failure to act, decision, or omission in order to improperly obtain, retain, or direct business to or to secure any improper benefit or advantage for **TAQA Group**. Examples of bribes include kickbacks, influence payments and **Facilitation Payments**.

Business

Any company or business within **TAQA Group**.

Business Day

Any day when banks are open for trading excluding weekends, and any days declared as public holidays in the applicable jurisdiction.

Business Leader

The appointed head of individual **Businesses** falling within the **TAQA Group.**

Business Partner

Includes any party with which **TAQA Group** conducts business, pays, or receives funds from, including (but not limited to) customers, suppliers, vendors, service providers, consultants, advisers, contractors, distributors, agents, commercial intermediaries, other intermediaries, investors, and partners and targets in a mergers and acquisitions context. It does not include those **Third Parties** acting only in their capacity as a **Retail Customer** or **TAQA Group Personnel**.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Business Partner Risk Assessment

The risk assessment carried out on a **Business Partner** by the respective **Business** using either their own internal **Due Diligence** process or using the **Business Partner Risk Assessment Score Sheet** pursuant to sections 3.1 and 3.4 of this **Business Partner Due Diligence Policy**.

Business Partner Risk Assessment Score Sheet

The risk assessment score sheet that may be used by any **Business** within the **TAQA Group** prior to doing business with a **Business Partner** (which may be updated from time to time).

Charitable Donations

A contribution of any kind to a recognized and legal charity by **TAQA Group** where the contributor does not receive any business related benefit in exchange (for example, a sponsorship promotion or branding rights). Donations of items that have zero book value are considered **Charitable Donations** under this Policy, provided they are given to a legal and recognized charity.

Closed Period

The statutory period during which any member of **TAQA Group Personnel** is prohibited from **Trading** in **TAQA Group Securities** under applicable law or regulation.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Civic Organization

An organization comprised of people who come together to provide a service to their community.

Commercial Sponsorship

Where an entity provides financial or in kind support for an event, person or organization by paying money or providing goods, services, or other consideration in return for the opportunity to promote that entity's brand and/or personnel or to access services, an event, or other marketing activities.

Commercially Sensitive Information

Any information which could be used by **TAQA Group** or its competitors to alter or align their commercial strategies. This includes but is not limited to confidential, non-public information in relation to prices or related topics (such as discounts or timing of price changes, margins, or overheads), bids, sales, market shares, customers, other trading conditions; allocation of customers or regions; capacity, supply terms or output; product cost information; strategic or marketing plans, R&D plans; the boycotting of competitors, suppliers or customers.

Competitor(s)

Individual persons or companies who actually, or may potentially compete with, **TAQA Group** in relation to the goods and services which **TAQA Group** offers or who provides similar goods and services. In certain circumstances, a **Competitor** may also be a **Customer**, **Supplier** or **Distributor** of **TAQA Group**.

Confidential Information

Information acquired in the course of activities for **TAQA Group** that:

(a) Relates to **TAQA Group's** business or a **Third Party**; and

(b) Is non-public or that **TAQA Group** indicates through its policies, procedures, or other instructions should not be disclosed to others.

Confidential Information could include information relating to **Customers**, **Suppliers**, partners, **TAQA Group Personnel** employees, business practices, financial results/expectations, prospective transactions, strategies, and investigations, and may consist of, among other things, documents, memoranda, notes, mailing lists, correspondence, and electronic records.

Controlled Item

An **Item** that is controlled for the purposes of applicable laws, rules or regulations, e.g. requires a **License** prior to export, re-export, transfer, or re-transfer.

Conflict of Interest (or Conflict)

Any situation in which a person, or **Related Person**, has a personal or external interest that is sufficient to appear to influence the objective exercise of judgement in official duties for **TAQA Group**, regardless of whether it would actually influence that exercise of judgement.

Counter Terrorist Financing (CTF)

Laws, regulations and guidelines designed to counter the financing of terrorist acts, terrorists, and terrorist organizations.

Corruption

An act done with an intent to give some improper advantage inconsistent with official duty and the rights of others; misuse of authority to secure some benefit either personally or for someone else contrary to duty and to the rights of others.

Customer(s)

Individuals or companies who purchases goods or receives services from **TAQA Group**. **Customers** might be end-users (e.g. final consumers), intermediaries (e.g. **Distributors**) or resellers excluding **Retail Customers**.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Data Protection Controller

An individual appointed by the respective **Business Leader** (who either alone, jointly or in common with other persons) determines the purposes for which **Personal Data** will be processed, and/or the means in which any **Personal Data** will be **Processed**, in order to implement this **Data Protection Policy.**

Data Protection Laws

Data protection laws that apply to **TAQA Group's Processing** of **Personal Data**, including any local laws and regulations that may apply in your jurisdiction in relation to handling personal information.

Data Protection Principles

the nine (9) data protection principles detailed in section 2 of this Policy.

Data Subject

An identifiable person who is the subject of **Personal Data**.

Director

A member of the governing Board of a corporation, association or other incorporated body.

Distributor(s)

Individual persons or companies who distribute **TAQA Group's** products or services.

DPIA

A data protection impact assessment.

Dual-Use Items

Items which can be used for both civil and military purposes and including all **Items** which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices. Different jurisdictions may provide specific definitions and requirements within their regulations.

Due Diligence

The process undertaken to assess risk by gathering, analyzing, managing, and monitoring information about an actual or potential **Business Partner**.

Entertainment

Includes, but is not limited to, attendance at plays, concerts, and sports events.

Enhanced Due Diligence

The process of undertaking additional steps to assess risk about an actual or potential **Business Partner** as described in this Policy.

Ethics & Compliance Office

TAQA Group's Ethics & Compliance Office.

EU GDPR

Regulation (EU) 2016/679 on the protection of natural persons regarding the **Processing** of **Personal Data** and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Executive Management

Any member of **TAQA Group Personnel** holding a senior management position (such as Chiefs, Directors (whether Executive or Non-Executive), VP's, etc.).

Facilitation Payments

Unofficial payment to a **Public Official** to expedite a routine function, which they are otherwise obligated to perform (e.g., visa processing, licenses, inspections etc.). A **Facilitation Payment** is a form of **Bribe**.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Family Member

A spouse, child, stepchild, grandchild, parent, stepparent, grandparent, sibling, mother- or father-in-law, son- or daughter-in-law or brother- or sister- in-law (including adoptive or custodial relationships) whether or not sharing the same household.

FCA

The Financial Conduct Authority established in the United Kingdom.

Financial Interest

Ownership of **Securities**, business property, or real estate (other than a personal or family residence), or any other type of financial relationship with a **Third Party**. A **Financial Interest** can be direct (held by the individual for his/her benefit) or indirect (held by someone else for the benefit of the individual, including through a trust or nominee).

Fraud

The intentional act of misrepresenting a fact to secure an unfair or unlawful advantage for business or personal profit, theft, the abuse of position or authority and the intentional and wrongful waste or destruction of property or resources.

GDPR

The **EU GDPR** and **UK GDPR**.

Gift

Anything of value, other than **Entertainment** and **Hospitality**, including, but not limited to, "courtesy gifts", payments (in the form of cash, checks, vouchers, gift cards, bank transfers, rebates or discounts not available to the general public), jewelry, food or beverage (outside of **Entertainment** and **Hospitality**), flowers, travel (outside of **Sponsored Travel**) and/or employment.

Government Entity

(a) Any national, state, regional or municipal government, (b) any supra-national body representing a collection of countries, e.g., the European Union; (c) any branch, agency, committee, commission, or department of any of the foregoing; (d) any person or organization authorized by law that performs any governmental, quasi-governmental or regulatory function; (e) any **Public International Organization**; (f) any political party; or (g) any state- owned or state-controlled enterprise.

Grant

A payment to a person or an organization for a particular purpose such as for education or research and development.

Hospitality

Includes, but is not limited to, refreshments, meals, and accommodation.

Insider

Any individual who is in possession of Material Confidential Information relating to Securities (including TAQA Group Securities).

Insider Trading

Buying or selling, in violation of applicable law, a publicly listed **Security** while in possession of **Material Confidential Information** about the company underlying that **Security**.

Investigation

The review and analysis of the factual, legal, and ethical bases of a concern, which may include interviews, reviews of documents and data, site visits, or receipt of advice from external advisors.

Investigator

Any person designated by the **Ethics & Compliance Office** to co-ordinate, supervise, and conduct the **Investigation** of a particular concern. This person may be internal to **TAQA** or external.

Item

Any goods, part, product, component, software, technology, or related **Technical Data**. Different jurisdictions may provide specific definitions and requirements within their regulations.

Know your Customer (KYC)

The internal process used to identify potential **Business Partners** as part of the **TAQA Group Due Diligence** process.

License

Authorization from the applicable Government(s) to export, import, re-export, re-transfer, or conduct any other regulated activity.

Lobbying

Individual or collective acts attempting to influence decisions made by governments, government officials, legislators, or other regulatory bodies.

LSE

means the London Stock Exchange established in London, England.

M&A Target

An organization or entity which is subject to a **Due Diligence** process with the potential for a merger or acquisition with **TAQA Group**.

Manager

A member of **TAQA Group** who is responsible for managing other members of **TAQA Group Personnel**.

Market Manipulation

Trading, distributing information, or otherwise behaving in a way that is likely to affect an investor's decision to invest in **Securities** by giving that investor a false or misleading impression about the supply, demand, price, or value of **Securities**.

Material Confidential Information

Any information, event, decision, or incident that: (a) relates directly or indirectly to a publicly listed company or its **Securities**; (b) is not publicly available; and (c) if it was publicly available, could affect the price of the relevant **Securities**, the movement or trading volume of those **Securities**, or an investor's decision to purchase, sell, or hold those **Securities**.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Money Laundering

The process criminals use to legitimize proceeds obtained from illegal activity. Money is "laundered" by passing it through lawful businesses or activities whilst the nature of the illegal financial transaction and the source, origin, and/or owner of the funds is hidden.

Monopoly

A market structure characterized by a single seller of a product within any given market where such seller is able to strongly influence or control market pricing and terms of sale.

Officer

A high-level management official of a business. Officers have the actual or apparent authority to contract or otherwise act on behalf of the business.

Overall Risk Classification

The **Overall Risk Classification** conducted pursuant to section 3.4 of this **Business Partner Due Diligence Policy**.

Personal Data

This is very broadly defined under **Data Protection Laws** and includes any information which relates to a living individual who can be identified, directly or indirectly, from that information. Examples of **Personal Data** are a person's name, address, date of birth, photographs, telephone numbers, email addresses, next of kin, passport details, IP addresses, location data, and bank and payroll information. These examples are not exhaustive.

Process/Processing/Processed

Has a very wide meaning under **Data Protection Laws** and includes obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) Organisation, adaptation or alteration of the information or data;

(b) Retrieval, consultation or use of the information or data;

(c) Disclosure of the information or data by transmission, dissemination or otherwise making available; or

(d) Alignment, combination, blocking, erasure or destruction of the information or data.

Political Contributions

Monetary or non-monetary contributions, such as resources and facilities, to support political parties, candidates, or initiatives.

Politically Exposed Person (PEP)

Persons who are or have been entrusted with prominent public functions and their immediate family members and persons known to be their close associate, including:

(a) A current or former:

  (i) Member of a royal family;

  (ii) Senior official in the executive, legislative, administrative, military, or judicial branch of a country or region (no matter whether elected);

  (iii) Senior official of a political party; or

  (iv) Senior executive of a government-owned commercial enterprise;

(b) A company, business, or other entity that has been formed by, or for the benefit of, any of the above;

(c) An immediate family member (including spouse, parents, siblings, children, and a spouse's parents and siblings) of any of the natural persons above; and

(d) A person who is widely and publicly known (or is actually known) to be a close associate of any of the natural persons above.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Public International Organization

A multinational institution made up of countries, governments, or other institutions that carries on any governmental or quasi-governmental activity(s) or function(s) such as the United Nations, the European Union or the World Bank.

Public Occasion

Any official public holiday or occasion (for example, in the United Arab Emirates, including Ramadan, Eid al-Fitr, Eid al-Adha and UAE National Day etc.).

Public Official

Includes any of the following:

(a) Official, employee, or person acting for or on behalf of any **Government Entity** or **Public International Organization**;

(b) Political party official or candidate for political office;

(c) Person who holds a legislative, administrative, or judicial position of any kind, whether elected or appointed, in a country or territory (or subdivision of a country or territory) or **Public International Organization**; or

(d) Person who otherwise exercises a public function for or on behalf of a country or territory (or subdivision of a country or territory) or for any public agency or public enterprise of a country or territory (or subdivision of a country or territory) or **Public International Organization**.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Related Person

In relation to **TAQA Group Personnel**:

(a) A spouse, civil partner, child, step-child, grandchild, parent, step-parent, grandparent, sibling, mother-in-law, father-in law, son-in-law, daughter-in-law, brother-in-law or sister-in-law, uncle, aunt, niece, nephew, or cousin (including adoptive relationships), whether sharing the same household or not;

(b) **Businesses** in which you are a general partner, owner (direct or indirect), or make management decisions;

(c) Trusts for which you are a trustee;

(d) Estates for which you are an executor; and

(e) Any other person or entity whose transactions are directed by, or subject to, your direct or indirect influence or control.

Retail Customers

TAQA Group's water and electricity-related retail customers in the United Arab Emirates.

Restricted Person(s)

Any member of **TAQA Group Personnel** who is a member of Executive Management, or otherwise has the power to make managerial decisions affecting the future development and business prospects of **TAQA Group**.

Sanctions

Limitations enacted by Governments or **Public International Organizations** that place restrictions on trade, economic, or financial activity, with specific countries, entities and persons.

Sanctioned Countries or Sanctioned Country

Countries and/or territories which are subject to comprehensive country- and/or territory-wide **Sanctions**.

Sanctioned Persons

Persons, entities or any other parties (a) located, domiciled, resident, or incorporated in a **Sanctioned Country**; (b) targeted by any **Sanctions** administrated by the United Nations, the European Union, the US, the UK, Japan, Canada, the United Arab Emirates and/or any other applicable country; and/or (c) owned or controlled by or affiliated with persons, entities, or any other parties as referred to in (a) and (b).

Sanctions Screening

The **Sanctions**-related screening procedure described in the **Business Partner Due Diligence Policy**.

Security(ies)

Equity, debt, and derivative financial instruments, including common shares, preferred shares, options, derivatives, swaps, futures, forwards, warrants, short positions, profit interests, convertible notes, bonds, notes, debentures, commercial paper, loan participations, limited partnership units, and other types of equity, debt, hybrid, and other securities including any **TAQA Group Securities**.

Special Category Data

Personal Data consisting of, or revealing in relation to, a **Data Subject** among other things:

(a) Race or ethnicity;

(b) Political opinions;

(c) Religious or philosophical beliefs;

(d) Trade union membership;

(e) Genetic data;

(f) VBiometric data for the purpose of uniquely identifying a natural person;

(g) Physical or mental health or condition; or

(h) Sex life or sexual orientation.

Please note that **Personal Data** relating to criminal convictions and offenses is also subject to enhanced protection under **Data Protection Laws**

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Sponsored Travel

Includes any form of transportation (such as airline tickets and taxis) and associated **Hospitality** and accommodation (such as hotel bookings) that is offered as part of a business-related engagement, such as conferences, site visits, or business meetings, and other than any such Travel or **Hospitality** provided for in any formal legal agreement.

Supplier(s)

Individual persons or companies who supply goods or services to **TAQA Group**.

Supervisory Authority

The relevant regulator in your jurisdiction with responsibility for data protection matters. For example, the **Supervisory Authority** in the United Kingdom is the Information Commissioner's Office.

TAQA

Abu Dhabi National Energy Company PJSC.

TAQA Group

Abu Dhabi National Energy Company PJSC **(TAQA);** any entity, operation, or investment controlled by **TAQA**, and/or any entity, operation, or investment, that adopts the **Code of Ethics & Business Conduct.**

TAQA Group Personnel

All individuals who work directly for or represent **TAQA Group**, including **Directors**, officers, employees, consultants, secondees, and contractors.

TAQA Group Securities

Any listed **Securities** issued or guaranteed by any member of **TAQA Group**, including without limitation any equity, debt, and derivative financial instruments, including common shares, preferred shares, options, derivatives, swaps, futures, forwards, warrants, short positions, profit interests, convertible notes, bonds, notes, debentures, commercial paper, loan participations, limited partnership units, and other types of equity, debt, hybrid, and other securities whether listed in the United Arab Emirates or elsewhere in the world.

Technical Data

Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, modification, use, installation, overhaul, or refurbishing of **Items**. Information may be in the form of blueprints, drawings, photographs, plans, instructions, diagrams, models, formulae, tables, engineering designs and specifications, manuals and documentation no matter in what form or media.

Terrorist Financing

The financing of terrorist acts, terrorists, and terrorist organizations.

Third Party

Any organization, entity, individual, or group other than **TAQA** or any of its **Businesses**, including any competitor, **Supplier**, affiliate, or **Customer** of **TAQA** or its **Businesses**.

Trade Controls

Prohibitions or restrictions on the trade or movement of goods, products or services from, to or through a particular country, imposed by the government or relevant authority of a country. Restrictions may be imposed over direct and indirect imports, exports, re-exports, transfers, and re-transfers in respect of (a) particular kinds of goods, products or services; (b) the exporting or destination country or geographic territory; and/or (c) the identity of the exporter or recipient.

Trading (including Trade, Traded or Trades)

Any type of transaction in Securities, including purchases, sales, the exercise of options, the receipt of shares under share plans, using Securities as security for a loan or other obligation, and entering into, amending or terminating any agreement in relation to Securities.

Trading Day

A day on which the stock exchange where the relevant **TAQA Group Securities** are **Traded** is open for **Trading**.

UAE Competition Authority

The Competition Authority within the Ministry of Economy of the UAE.

UAE Competition Law

Federal Law No. 4 of 2012 Concerning Regulating Competition.

UK GDPR

Regulation (EU) 2016/679 on the protection of natural persons with regard to the **Processing** of **Personal Data** and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as it forms part of retained EU law.

Unless noted otherwise, definitions cover the singular and plural number of any defined term.

Revision History

Speaking Up Policy

Version No: 2.0

Issue No: 1

Issue Date: March 2021

Conflicts of Interest Policy

Version No: 2.0

Issue No: 1

Issue Date: March 2021

Anti-Bribery & Corruption and Anti-Fraud Policy

Version No: 2.0

Issue No: 1

Issue Date: March 2021

Insider Trading Policy

Version No: 2.0

Issue No: 1

Issue Date: March 2021

Data Protection Policy

Business Partner Due Diligence Policy

Anti-Money Laundering Policy

Sanctions and Trade Controls Policy

Antitrust Policy