

CODE OF ETHICS



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

LEADERSHIP MESSAGE



Together, we can ensure that the Mubadala Group is immediately recognized by our impeccable ethical conduct in everything that we do, wherever we are



As a global investment company with a mandate to generate sustainable financial returns for our shareholder, the Government of Abu Dhabi, this Code of Ethics reflects both the standards we expect of ourselves and the high expectations of our shareholder. It is intended to enable us to achieve our commercial goals while operating with the highest levels of integrity.

The Code serves as the foundation for a culture that fosters actions consistent with our ethical standards. It reminds us that ethics requires action; it cannot be instilled through a document, nor can it exist separate from our words or conduct.

Together, we can ensure that the Mubadala Group is immediately recognized by our impeccable ethical conduct in everything that we do, wherever we are.

Khaldoon Khalifa Al Mubarak
Managing Director & Group Chief Executive Officer
Mubadala Investment Company



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions

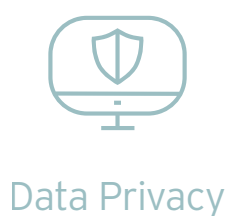


Policy Details

2

/ 60





INTRODUCTION

This Code sets out the basic principles, standards and behaviors necessary to achieve our objectives and uphold our values. It makes clear that we not only follow the law but strive to operate with the highest levels of ethics and integrity.



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



To whom does the Code apply?

This Code applies to everyone who works directly for or represents the **Mubadala Group**, including all employees and Directors of Mubadala and its controlled subsidiaries. We also require our contractors, partners, consultants and suppliers to adhere to the **Business Partner Code of Conduct**.

This Code is supplemented by a number of policies which offer further detailed guidance. Although we strive to provide clear guidance regarding our ethical obligations, no policy can ever cover every scenario. The absence of guidance to deal with a particular situation does not relieve us from the responsibility to act consistently with the law and highest ethical standards of business conduct at all times. Where there is no specific guidance on a particular matter, always seek help from the **Ethics & Compliance Office**.

Who manages the Ethics & Compliance program?

The Mubadala Board of Directors is responsible for ensuring that there is an effective ethics and compliance program in place. At the direction of the Board, the Managing Director & Group CEO established an independent Ethics & Compliance Office to develop, coordinate and support the ethics and compliance program across the Mubadala Group. The Ethics & Compliance Office reports functionally to the Board's Audit, Risk & Compliance Committee and has direct access to and support from the Ethics & Compliance Review Board, which consists of Mubadala's most senior executive management.

What is the role of the Ethics & Compliance Office?

The Ethics & Compliance Office leads, develops and supports all aspects of the Mubadala Group ethics and compliance program. Its responsibilities include, among other things:

- Empowering a culture of ethics and compliance
- Ensuring everyone, especially Leadership, is committed to ethical conduct

- Creating and administering a comprehensive ethics and compliance program, designed to prevent unlawful or unethical business conduct, and to detect it if it occurs
- Assessing ethics and compliance risks and testing to ensure that internal controls are responsive to those risks
- Investigating and remediating alleged violations of law, regulation or policies and procedures, and ensuring that improper conduct is held consistently and fairly to account

What is your Role?

- Ethics and compliance is the responsibility of everyone. By working for, or with, the Mubadala Group, you are agreeing to fulfil these responsibilities and adhere to our Code and values. Those who fail to follow our Code put themselves, their colleagues, and the entire Mubadala Group at risk
- It is your responsibility to read, understand and adhere to this Code and any related policies and procedures. Violation of this Code may result in disciplinary action, including up to termination of your employment and/or criminal or civil sanctions
- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times, and expect the same from others
- Understand and comply with the requirements of this Code and other Ethics & Compliance policies
- Provide appropriate resources and support to ensure the successful implementation of this Code
- Complete assigned training relating to this Code



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

OUR CODE OF ETHICS AT A GLANCE

- ✓ We are committed to a culture of ethics and compliance by which we conduct our global business with integrity and in accordance with applicable laws, rules and regulations
- ✓ We encourage you to speak up when you see or suspect violations of the law, rules, regulations, policies or this Code of Ethics
- ✓ We treat everyone with respect and do not tolerate unfair treatment, harassment, discrimination, abuse or retaliation within the workplace
- ✓ We protect sensitive, confidential and Material Non-Public Information and Personal Data
- ✓ We carefully select our customers, partners and suppliers and require that they conduct their business activities professionally, ethically, and in compliance with applicable laws, rules and regulations
- ✓ We offer and accept Gifts and hospitality that are reasonable and appropriate, follow global Anti-Bribery and Corruption laws, and avoid the appearance of any conflict of interest that might violate applicable laws or harm relationships or reputations
- ✓ We are mindful in forming strategic partnerships with Governments and of the special risks and responsibilities those relationships carry
- ✓ We protect our assets and reputation by observing internal controls and recognized financial and accounting practices
- ✓ We follow international commercial laws and standards, including intellectual property protections, prohibitions on Insider Trading and anti-competitive conduct, and provisions governing imports, exports, and international trade



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

5

/ 60

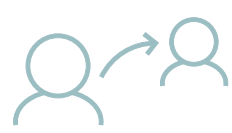




Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



CULTURE

- ▶ Integrity
- ▶ Speaking Up
- ▶ Respect & Fairness



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

6

60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

INTEGRITY

Values are the foundation of our culture, leadership is its architect, and we are its engineers

What to Know:

- Integrity is the principle that gives us a common purpose and provides direction on how we should conduct ourselves
- Our commitment to integrity has meaning and effect only when we act consistently with it, reiterate it frequently, facilitate an open dialogue about it, and enforce accountability for it
- The behaviors we allow are the behaviors we encourage, and the practices we reward are the practices that will be repeated
- The sum of our values, behaviors, and practices is our culture
- We look to our leaders to model ethical workplace behavior and to shape the right culture in the workplace

What to Do:

- Exhibit ethical behavior and speak openly and frequently about the role of integrity in the workplace
- Align incentives to reward performance with integrity, rather than performance at any cost
- Promptly report any breaches of this Code to the Ethics & Compliance Office

WATCH OUT FOR:

- The temptation to assume that our values and culture exist apart from our words and actions
- People who resist, rather than support, our culture and commitment to integrity



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

7

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

SPEAKING UP

Ethics and compliance is the responsibility of everyone. Anyone who believes a law, rule, regulation, policy or this Code has been, or is being, violated or witnesses other unethical workplace conduct, should speak up

What to Know:

- We encourage openness and ask everyone to raise ethics or compliance questions or concerns in good faith, without fear of retaliation - even if they turn out to be mistaken
- You are also able to raise a question or report a concern anonymously
- Those who engage in retaliatory action against anyone who reports an issue will be subject to disciplinary action
- Confidentiality is key to protecting you and the investigative process; information will only be disclosed strictly on a need-to-know basis
- Intentionally false, exaggerated reports, and reports made in bad faith will not be tolerated and those who make these reports may be subject to disciplinary action

What to Do:

- Raise concerns in good faith. Refrain from raising concerns simply because you have personal or workplace differences
- Do not worry about the consequences of reporting a concern. No one will suffer any penalty or other adverse consequences from good faith and genuine reporting of possible wrongdoing, even if we lose business or suffer financial or other disadvantage as a result
- Where possible, try to resolve directly any workplace interpersonal issues that you might have, or raise them with Human Capital or a manager, before raising your concern formally
- Cooperate with investigations when requested, so that matters are quickly and properly resolved
- Respect the confidentiality of investigations. Refrain from sharing information about an investigation, except as directed. Do not expect to learn the outcome of an investigation unless you will be implementing or assisting with follow-up actions
- If you see it, say it!



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

RESPECT & FAIRNESS

Our strength lies in the talent and diversity of our people, so we must respect everyone's right to dignity

What to Know:

- We do business in a number of countries and across a spectrum of cultures
- We must treat each other respectfully and fairly, and not tolerate any form of harassment, abusive, or offensive behavior
- Be able to identify the various forms of harassment which might include, amongst others, bullying, discrimination, intimidation, physical violence, and sexual harassment
- We abide by applicable international human rights principles
- We comply with all applicable laws, rules and regulations, including those in relation to employment practices
- We provide a safe and healthy workplace for all employees
- We do not use, employ, or seek to exploit in any way the services of child, under-aged, slave or trafficked labor

What to Do:

- Treat everyone with respect and dignity - never threaten, humiliate, discriminate or use suggestive or disparaging language or actions, including in the context of critical feedback
- Respect the cultural standards, both of the country where you work and of the people with whom you work
- Ensure all employment-related decisions, e.g., hiring, promotion, etc., are carried out fairly, legally, are consistent with relevant processes, and are based on merit and the needs of the business
- Report any concerns pertaining to Respect & Fairness to the Ethics & Compliance Office

WATCH OUT FOR:

- Encroaching on others' personal space or unwanted physical contact
- Discrimination or harassment of any sort



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

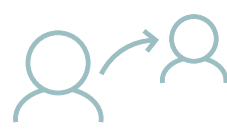
9

/ 60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



INTERNAL BUSINESS CONDUCT

- Conflicts of Interest
- Asset Management & Controls



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

10

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

CONFLICTS OF INTEREST

We require any activities outside work, whether financial, business, or otherwise, to be lawful. They should not compromise or interfere with - or even appear to do so - your workplace objectivity and responsibilities

What to Know:

- A **Conflict** arises if financial, business, social activities, or personal relationships interfere with or influence, or appear to interfere with or influence, your workplace objectivity or your role with the Mubadala Group
- **Conflicts of Interest** resulting from us possessing business or financial ties to third-party stakeholders could create business risks and may be subject to scrutiny
- Using the Mubadala Group as a platform to directly advance personal interests (business or otherwise), or to benefit Related Persons and or third parties, is an unacceptable Conflict of Interest
- We require you to declare and seek approval for any potential or actual Conflict of Interest, or to certify that you have no such Conflict

What to Do:

- Be familiar with and understand the disclosure requirements of the **Conflicts of Interest Policy** and ask questions to the Ethics & Compliance Office if you require further clarity
- Avoid any activity that creates a conflict, or even the appearance of a Conflict, between your personal interests and the interests of the Mubadala Group
- Disclose any actual, perceived, or potential Conflict of Interest that you might have in order to protect yourself and the organization
- Follow any restrictions imposed on you as a result of a Conflict of Interest disclosure
- Raise any questions and report any concerns pertaining to Conflicts of Interest to the Ethics & Compliance Office

WATCH OUT FOR:

- Personal relationships with current or potential competitors, customers or suppliers of the Mubadala Group
- The blurring of lines between any outside activities and your Mubadala Group employment
- Hiring, promoting or supervising a Related Person



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

11

/ 60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

ASSET MANAGEMENT & CONTROLS

We rely on our policies and procedures to set our organizational standards, and we abide by them to comply with applicable laws and regulations, as well as financial and accounting standards

What to Know:

- Delegations of Authority establish decision-making authority on behalf of a company. Acting outside your authorization may lead to disciplinary action
- Following the correct procurement and legal contracting processes maximizes value and protects the organization
- We require accurate and consistent recording of financial and business information, complying with relevant reporting standards
- We have zero tolerance for **Fraud** or any similar illegal act characterized by deceit, concealment or violation of trust to obtain money, property or services; or to secure personal or business advantages
- Misrepresenting facts or financial information, or misappropriating company assets for personal use, could be considered Fraud or theft and can lead to civil and/or criminal penalties and/or disciplinary action

- Theft of or damage to our property, or that of our colleagues or third parties, will not be tolerated, and may result in legal and/or disciplinary action

What to Do:

- Know and stay within your authority under the relevant Delegation of Authority
- Always engage Legal & Governance and Procurement when contracting with a third party
- Before signing or forwarding a document containing your signature, confirm your authority and verify the facts for accuracy and completeness
- Report any concerns pertaining to Asset Management & Controls or any indications or suspicions of financial misstatement, Fraud, theft, or other misconduct to the Ethics & Compliance Office

WATCH OUT FOR:

- Requests for sign-off and processing of important documents, such as agreements or contracts, that are rushed or expedited without justification
- Manipulation of a Delegation of Authority or Procurement process for personal gain or through negligence



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

12

/

60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



EXTERNAL RELATIONSHIPS

- ▶ Anti-Bribery & Corruption
- ▶ Working with Governments
- ▶ Business Partners



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

ANTI-BRIBERY & CORRUPTION

We permit the exchange of certain Gifts and hospitality in the professional environment when they are modest and appropriate under the circumstances. However, we avoid any activity that might give rise to Bribery or Corruption or the appearance of these activities

What to Know:

- Global Anti-Corruption laws define a “bribe” broadly, and those definitions include conduct that may be acceptable under many circumstances but is unacceptable when combined with an attempt to improperly influence a business-related decision
- Items of value that could be considered to be a bribe include (but are not limited to) cash, gift cards, vouchers, gifts, travel, entertainment, hospitality, internships, employment, housing, loan repayments, and certain charitable or political contributions
- **Bribes**, kickbacks, unfair advantages, and other acts of corruption are strictly prohibited
- You cannot make or receive a **Facilitating Payment** or any other form of improper payment

What to Do:

- Never offer, give or accept payment or anything of value (such as a Gift) directly or through a third party, in the attempt to gain business or to improperly influence a business decision
- Only offer and receive Gifts, Entertainment and Hospitality in line with our **Anti-Bribery & Corruption Policy**
- You must contact the Ethics & Compliance Office if you are, or believe you may be, confronted with a Bribe or potential Facilitating Payment
- Report any concerns pertaining to **Bribery** or Corruption to the Ethics & Compliance Office

WATCH OUT FOR:

- Third-party consultants who do not clearly describe their work, account for their expenditures, or whose commissions seem unjustified in the context of the services provided
- Anyone who hints or suggests that certain payments be made to obtain business or information



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

14

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

WORKING WITH GOVERNMENTS

We are mindful of the special precautions that must be taken when interacting with Government Entities or Government Officials

What to Know:

- We invest, partner and interact with **Government Entities** around the globe
- Business practices, such as hospitality, that may be acceptable in the commercial arena may be unacceptable, illegal or viewed as potentially corrupt in Government business
- Government dealings receive extra scrutiny, and even the allegation of corruption can result in serious reputational damage
- We do not involve the Mubadala Group, directly or indirectly, with any form of political or electoral activity. Any lobbying activities must be legal, for legitimate reasons and ethical

What to Do:

- Understand and comply with laws governing commercial interactions with Governments in the countries in which you operate or do business
- Take special care when exchanging Gifts, entertainment or hospitality with **Government Officials**, including personnel of state-owned or state-controlled entities
- Ensure the accuracy and completeness of financial and other information related to Government Entities and representations, certifications or filings provided to Government Entities
- Notify the Ethics & Compliance Office of any investigations, audits, or unusual requests for data by any Government Entity
- Ensure that your personal political or electoral activities represent you personally and do not suggest a connection to the Mubadala Group
- Report any concerns pertaining to Working with Governments to the Ethics & Compliance Office

WATCH OUT FOR:

- The use of agents who have direct interactions with Governments
- Local or regional hospitality practices that are not aligned with global anti-corruption standards, particularly when Government Officials are involved



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

15

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

BUSINESS PARTNERS

Business Partners play an integral role in our business. We evaluate them carefully before engaging with them, and we expect them to conduct themselves in an ethical and compliant manner

What to Know:

- **Business Partners** are expected to comply with applicable laws and regulations, act according to our standards in relation to ethics, integrity and compliance, and comply with our **Business Partner Code of Conduct**
- All Business Partners must be vetted, particularly those that interact with Governments on behalf of the Mubadala Group
- Business Partners must be subject to confidentiality agreements if they have access to sensitive, confidential, Material Non-Public Information, or proprietary information
- Business Partners should be selected fairly and without any conflict of interest or any kind of favoritism that might compromise the selection process
- Business Partners should treat workers fairly, provide a safe and healthy workplace, minimize their environmental impact and impose the same requirements on their subcontractors
- We do not engage in and/or facilitate **Money Laundering** and **Terrorist Financing** in any way whatsoever

What to Do:

- Know your Business Partners and conduct necessary risk-based Due Diligence in accordance with our **Business Partner Due Diligence Policy** to reasonably assure yourself that their business activities and transactions are legal, reputable and responsible
- Ensure you understand and can describe the services provided by any Business Partner for which you are responsible
- Be alert to any payments that look irregular, funds from or to dubious or unknown sources, or customers who appear to lack integrity in their operations
- Do not conduct business with an anonymous or fictitious company, or with any Business Partner whose identity or business activities are unclear or unknown
- Choose Business Partners based on merit and in line with procurement policies and processes
- Obtain commitments from your Business Partners to conduct themselves in an ethical and compliant manner consistent with our **Business Partner Code of Conduct**
- Report any concerns pertaining to Business Partners to the Ethics & Compliance Office

WATCH OUT FOR:

- Funds paid from or to companies that do not appear to be affiliated with the Business Partner or from/to countries not normally associated with the Business Partner
- Any Business Partner who provides incomplete, suspicious or overly complicated information
- Third parties who hold themselves out as acting for Mubadala Group in the absence of an agreement documenting the scope and terms of their mandate



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

16

/

60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



MARKETPLACE CONDUCT

- ▶ Insider Trading
- ▶ Intellectual Property, Fair Competition & Commercial Information



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

17

60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

INSIDER TRADING

We observe laws that protect the integrity of securities markets and take steps to prevent market misconduct

What to Know:

- **Material Non-Public Information** (also referred to as 'inside information') is information that (a) is of a precise nature; (b) relates directly or indirectly to a publicly listed company or any company with a publicly listed **Security(ies)**; (c) has not been disclosed to the public by that company and is not otherwise in the public domain; and (d) would, if it were made public, be likely to have a significant effect on the price of those Security(ies)
- **Insider Trading** is buying or selling (whether directly or indirectly) any Security personally or through a Related Person or others while in possession of Material Non-Public Information about the company underlying that Security
- **Securities Tipping** is disclosing Material Non-Public Information to enable another person to buy or sell a Security on the basis of that information
- Individuals involved in market misconduct will be subject to disciplinary action and may be subject to criminal and/or civil proceedings
- If you serve as a Director of a publicly listed company, you must obtain written approval, and must confirm appropriate information barriers are in place, before sharing internally or externally any non-public information obtained from your role as a Director

What to Do:

- Do not engage in any form of market misconduct
- Do not discuss or disclose any **Material Non-Public Information** inside or outside the Mubadala Group without necessary approvals
- Continually monitor and observe any restrictions that may be imposed on your personal Securities
- Complete any required disclosures related to your personal Securities trading activities in accordance with our **Personal Trading Policy**
- Report any concerns pertaining to market misconduct to the Ethics & Compliance Office

WATCH OUT FOR:

- Trading activity that takes place around the same time as a significant announcement concerning that company
- Discussing with Related Persons and/or unauthorized third parties Confidential Information related to a company that is listed on a publicly traded exchange



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

18

/ 60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

INTELLECTUAL PROPERTY, FAIR COMPETITION & COMMERCIAL INFORMATION

We use and gather commercial information fairly, respect **Intellectual Property (IP)** rights and promote fair competition

What to Know:

- **Intellectual Property (IP)** laws protect certain information in the public domain, such as trademarks and patents, as well as some proprietary information, such as business plans and trade secrets
- Antitrust and competition laws prohibit certain agreements between, or information sharing among, competitors or businesses within the same supply chain. They also impose onerous disclosure requirements in connection with certain types of agreements
- Legitimate sources of competitive information include such things as publicly available literature and industry publications
- Gathering information about competitors by theft, misrepresentation, eavesdropping, inducement or similarly illegitimate means is never acceptable

What to Do:

- Respect the IP rights of others and protect our own IP rights within the Mubadala Group
- Do not enter into any discussions with competitors to exchange or share sensitive, competitive or Material Non-Public Information, such as profits or market share
- Only collect and use information in a lawful manner
- Involve Legal & Governance when negotiating agreements to ensure they are consistent with competition laws and that all necessary disclosures are made
- Report any concerns pertaining to IP rights, Fair Competition or Commercial Information to Legal & Governance

WATCH OUT FOR:

- Discussions at meetings or industry events where any competitor attempts to discuss competitive information
- Internal discussions regarding market share or of a desire to dominate a particular market
- Use of trademarked names or patented technology not belonging to us, without knowing whether appropriate licensing agreements are in place



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

19

/ 60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



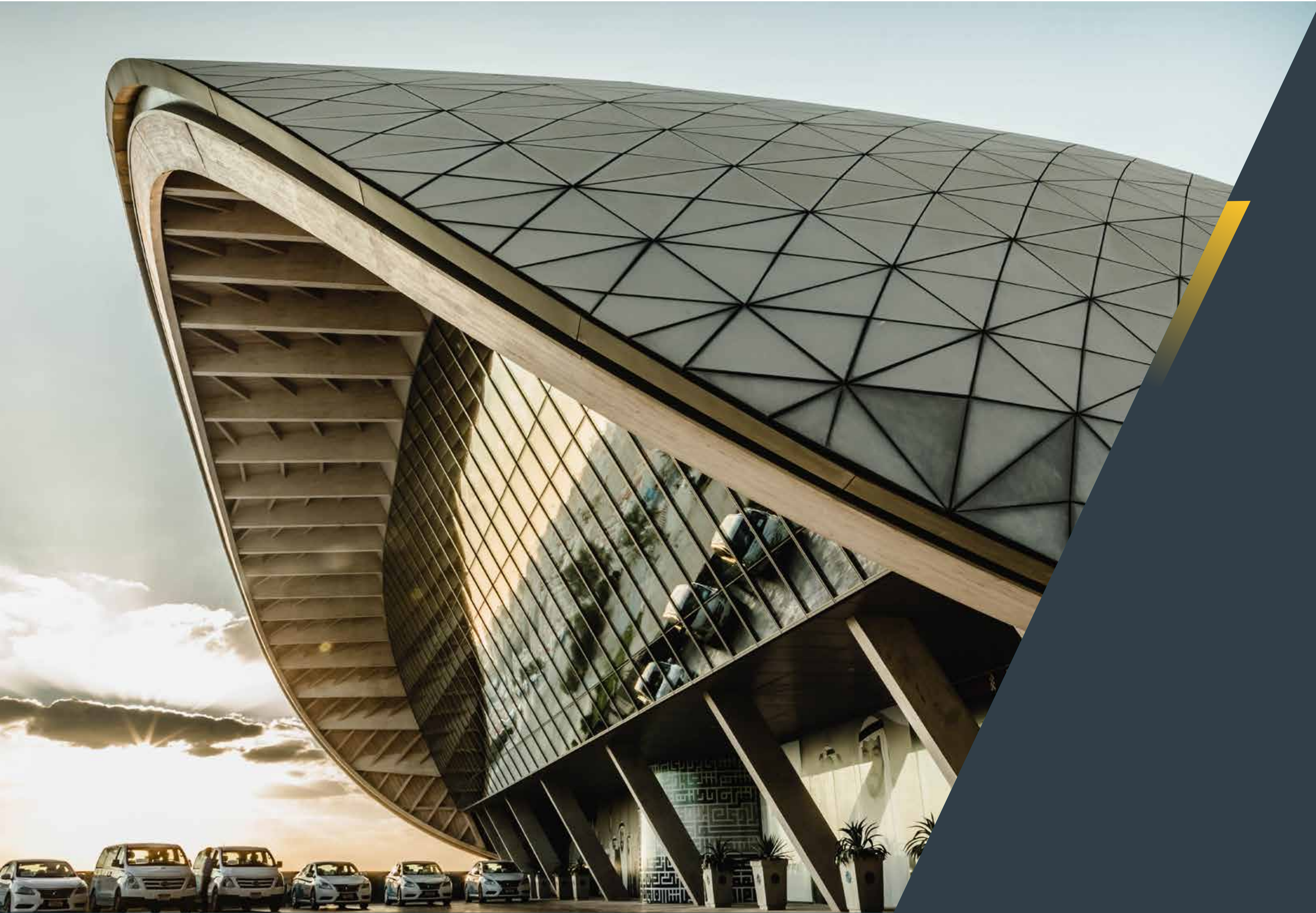
E&C Artificial Intelligence



Contact Us



Last viewed page



INFORMATION

- ▶ Confidentiality & Data Privacy
- ▶ Information Management & Communications
- ▶ Information Technology



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

20

60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

CONFIDENTIALITY & DATA PRIVACY

We recognize the critical role of confidentiality in an information-based world and we protect sensitive, confidential and Material Non-Public Information both when it is our own and when we act as stewards of others' information

What to Know:

- Much of the information we encounter in our jobs may be confidential to varying degrees. Properly managing that information is a core responsibility we all share
- Mismanagement or misuse of sensitive, confidential or Material Non-Public such as Insider Trading, breach of data privacy laws, unlawful anticompetitive agreements, or Intellectual Property law violations can result in potentially serious consequences, including criminal penalties
- Personal Data receives special protection in many jurisdictions. Those protections limit how we use the information, and where and with whom we can share such information. Data privacy law violations can result in potentially serious consequences, including regulatory sanctions
- We respect the privacy of our colleagues' personal information, and limit access to personal records to those with appropriate authorization

What to Do:

- Safeguard Confidential Information in your possession, whether it belongs to us or a third party
- Ensure appropriate legal and logistical protections are in place before you accept Confidential Information from anyone outside the Mubadala Group or share any Personal Data or non-public information internally or externally
- Protect all forms of Personal Data in your possession in accordance with our **Data Privacy Policy**
- Report any concerns relating to Confidentiality & Data Privacy to the Ethics & Compliance Office

WATCH OUT FOR:

- Discussing Confidential Information with third parties in the absence of a non-disclosure agreement
- Transferring Personal Data, including collections of data that may include names and email addresses, between companies or across borders



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

INFORMATION MANAGEMENT & COMMUNICATIONS

We observe the necessary standards for information management and release communications only after vetting them with appropriate stakeholders

What to Know:

- “Document” is broadly defined and includes hardcopy and electronic records and communications, such as e-mails, text messages and voice recordings
- Many documents are subject to regulations that require their retention for a prescribed period of time
- Documents must receive appropriate confidentiality treatment and should be disposed of at the appropriate time
- External communications on behalf of the Mubadala Group must be accurate, timely, and fully coordinated with and approved by internal stakeholders before release

What to Do:

- Know which documents you have that must be retained, and for how long, and maintain them accordingly
- Do not dispose of any records that are subject to a legal hold notice, even if beyond the required retention period
- Know which of your communications on behalf of the Mubadala Group require authorization. Do not release such communications without obtaining the necessary approvals
- Report any concerns pertaining to Information Management & Communications to the Ethics & Compliance Office

WATCH OUT FOR:

- Discussing with Related Persons and/or third parties Confidential Information related to a company that is listed on a publicly traded exchange



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

22

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

INFORMATION TECHNOLOGY

The hardware, software, data, and networks that comprise our information technology (IT) resources are critical assets, and we are mindful of the prominent role of cybersecurity in today's global business environment

What to Know:

- Communications made using our IT assets, such as a computer, telephone, mobile device, SIM card, e-mail account, network or other electronic resource, and the information stored on them, are company property
- Where legally permitted, we may record communications and monitor activity across our IT assets to ensure those assets are used lawfully and in accordance with our policies and procedures
- E-mail communications, in particular, are often critical evidence in investigations and litigation
- Cyber attacks are a primary risk for businesses globally, and preventing them requires heightened awareness and vigilance by us all

What to Do:

- Use your IT assets properly, whether those devices are our IT assets or your personal devices used for business purposes
- Any personal use of our IT assets should be kept to a minimum. Never use our IT assets to engage in communications or access material or websites that are offensive, illegal, or obscene
- Protect our IT assets, the information they contain, and passwords from theft or unauthorized access
- Take proactive measures to protect our IT assets by flagging phishing links, screening external storage devices, and attending cyber security training and awareness sessions
- Report any concerns pertaining to IT to the Ethics & Compliance Office

WATCH OUT FOR:

- Emails, text messages or other electronic communications that contain suspicious information, inappropriate content, or solicitations from unknown sources
- Inappropriate use of social media websites that could cause reputational harm to the Mubadala Group through association or disclosure of any Confidential Information through such mediums



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

23

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



CONFLICTS OF INTEREST **POLICY**



Summary



Requirements



Definitions



Policy Details

24

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

POLICY SUMMARY

A **Conflict of Interest** arises when personal interests conflict with the interests of the **Mubadala Group**, or when judgement or decision-making is inappropriately influenced by outside interests.

Such **Conflicts** are either existing (actual), a situation that could result in a Conflict (potential), or a situation that could appear to be a Conflict but in fact is not (perceived).

You owe a primary duty to the Mubadala Group to advance its legitimate interests and not to advance your own personal interests at the expense of the Mubadala Group.

This Policy provides guidance to assist you in recognizing possible Conflict of Interest situations and on reporting them to the **Ethics & Compliance Office**.

Applicability & Consequences:

This Policy applies to the Mubadala Group and to **Mubadala Group Personnel**. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities.

Assets 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.

Your Responsibilities:

- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the **Mubadala Group Code of Ethics**, other Ethics & Compliance Policies, and any Corporate Unit/ Business Unit or Asset policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy

Questions & Reporting Violations:

Promptly report in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.

Failure to promptly report any known or suspected violations of this Policy to the Ethics & Compliance Office is itself a breach of this Policy and may result in disciplinary action.



Summary



Requirements

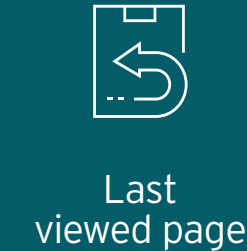


Policy Details

25

/ 60





POLICY REQUIREMENTS

You must be free from Conflicts that could adversely influence your judgement, objectivity, or loyalty in conducting business activities and assignments for the Mubadala Group. It is important that you maintain personal credibility by avoiding any activity that would bring into question your objectivity or loyalty to the Mubadala Group.

You should not threaten or retaliate against anyone who refuses to engage in activity prohibited by this Policy, or who raises concerns about possible wrongdoing under this Policy - even if we lose business or otherwise suffer a business disadvantage.

1. Conflicts of Interest Categories

Conflicts arise in many different ways, and the appearance or perception of a Conflict can often do as much harm as the actual existence of a Conflict. The following scenarios identify situations that you may face and must be disclosed as potential, actual or perceived Conflicts.

It is not possible to list every possible Conflict or potential Conflict situation, so it is important that you seek advice from the Ethics & Compliance Office for any help and support you may need.

a. Financial Interest in an Outside Concern

- i. Having a **Financial Interest** in a third party, competitor, supplier, affiliate or customer of the Mubadala Group or in an **Outside Concern** where you could personally affect the Mubadala Group's business with that Outside Concern
- ii. Having a Financial Interest of 1% or more of a

publicly-traded company within the Mubadala Group portfolio of investments

b. Holding a Position as Officer or Director in an Outside Concern

- i. Civic Organizations: Your support of a **Civic Organization**, or contributions of Mubadala Group time and resources to it, can result in a Conflict even where no personal gain or economic interest is involved. You must disclose such arrangements and ensure that Due Diligence has been conducted to understand your legal and fiduciary liabilities and responsibilities
- ii. Government Entities: If you are asked to serve as an **Officer** or Director of a **Government Entity**, you must disclose any such requests prior to accepting them to ensure that your appointment will not appear to conflict with your obligations to the Mubadala Group
- iii. Commercial organizations: Having a position of Officer, Director, or other management position in an Outside Concern must be disclosed if the organization is a competitor to, conducts business with, or seeks to conduct business with the Mubadala Group
- iv. Advisory Boards: Serving on an **Advisory Board** or "user group" for an Outside Concern must be disclosed because it may create the impression that you are being rewarded for granting business to the Outside Concern or that it is attempting to influence your decisions made in relation to the Mubadala Group





c. Other Associations with Outside Concerns

- i. Local sponsors or national services agents: You must disclose any Outside Concerns you sponsor, directly or indirectly, if they do business with or seek to do business with the Mubadala Group
- ii. Other services for an Outside Concern: You must disclose services or support provided to an Outside Concern if such activities could impact the proper performance of your duties for the Mubadala Group - including conflict of time commitments or potential conflict for reputational harm to the Mubadala Group

d. Employment

- i. Making decisions or being in a position to have direct authority or influence over the hiring, promotion, salary and financial and/or procurement decisions of a Related Person
- ii. Taking any outside employment, including a parttime job, or providing consulting services to any entity or acting as an independent consultant, whether the entity is doing or seeking to do business with or competing against the Mubadala Group
- iii. Using Mubadala Group facilities, equipment, IT resources, and time for part-time employment or other outside consulting or business activities

e. Related Persons

- i. Employment of a Related Person at the Mubadala Group
- ii. Having a Related Person employed by an entity seeking to do or doing business with the Mubadala Group
- iii. Directing Mubadala Group associated business to any entity that is owned, sponsored, or managed

by a Related Person

- iv. Using Mubadala Group equipment, resources, or materials for a business owned or sponsored by a Related Person
- v. Any relationship that may create a Conflict with your Mubadala Group responsibilities or compromise Mubadala Group interests

f. Use of Confidential Information or Mubadala Group Resources

Confidential Information belonging to us or managed by us for customers, suppliers, partners, and employees must be adequately protected and managed. Similarly, our equipment, technology, and resources must be secured and used appropriately. You must avoid any Conflict of Interest resulting from the following:

- i. Use of Mubadala Group Confidential Information in an Outside Concern
- ii. Using Mubadala Group facilities, equipment, IT resources, and time for part-time employment or other outside consulting or business activities
- iii. Misuse of Mubadala Group resources, your position, or influence to promote or assist an Outside Concern
- iv. Mishandling of competitive Confidential Information to gain personal benefit

g. Procurement

- i. If you are referring a supplier and/or asked to participate in the review, selection, award, and/or administration of a contract where there may be an actual, potential or perceived Conflict of Interest with a supplier, bidder or interested party
- ii. Soliciting our suppliers, customers, or other business relationships that may be associated with

the Mubadala Group for donations to a charity or Civic Organization in which you are personally involved must be disclosed and approved before any such approach or request is made

2. Conflicts of Interest Disclosure Process

To enable us to manage situations that may arise in respect to business and personal Conflicts, you are required to disclose actual, potential and/or perceived Conflicts to the Ethics & Compliance Office by completing the Conflict of Interest disclosure form located on the Ethics & Compliance Office intranet at <https://ethics.mubadala.ae>.

As part of the annual Code of Ethics acknowledgement you will also be required to submit a declaration confirming that you have disclosed any and all Conflicts.

When a Conflict is disclosed, the Ethics & Compliance Office will review the disclosure and consult with your line manager and/or **Business Leader** to determine the appropriate course of action. The Ethics & Compliance Office will then inform you whether the situation is considered a Conflict, and, if so, whether it is one that can be managed. If your situation presents a manageable Conflict, you will be advised on how to manage it, including specific recommendations and actions that you must follow. It also may be necessary to engage other stakeholders depending upon the type of disclosure.

A disclosure may be rejected if the situation is unmanageable. If you delayed or neglected submitting or updating a disclosure or breached any associated condition, the disclosure may also be rejected and you may be subject to disciplinary action.

The disclosure request is not considered closed until a final response from the Ethics & Compliance Office is provided. You are also required to notify the Ethics & Compliance Office of any changes or updates to any initial Conflict of Interest disclosure(s).



ANTIBRIBERY & CORRUPTION POLICY

POLICY SUMMARY

We are committed to conducting business in accordance with the highest ethical standards and prohibit all forms of Bribery and Corruption. **Bribery** and **Corruption** are illegal in most countries and may take various forms: from the obvious (e.g., cash bribes) to the subtle (e.g., job offers, internships, commissions, lavish hospitality, etc.). Subtle forms of Bribery and Corruption often sit in grey areas. For instance, not every job offer is a **Bribe**, and not every commission is a corrupt payment – but they could be.

This Policy sets out guidance on how to prevent improper payments and to help provide a structure to ensure accurate reporting of all payments under applicable Anti-Bribery and Corruption laws.

In summary, you:

- Are prohibited from offering or receiving Bribes, a **Facilitating Payment** or any other form of improper payment
- May participate in legitimate business activities, such as receiving and offering **Gifts, Entertainment & Meals, Sponsored Travel & Hospitality** and **Sponsorships** – so long as they comply with this Policy
- Must request pre-approval from your **Business Leader** and the **Ethics & Compliance Office** for activities covered by this Policy, in accordance with the relevant thresholds as follows:

Pre-approval requirements (giving to / receiving from)			
	Government Official/Entity	Commercial Entity	Mubadala Group
Gifts	Any value	>= AED 550 (USD 150) per person/per event	No approval needed
Entertainment & Meals	Any value	>= AED 550 (USD 150) per person/per event	No approval needed
Sponsored Travel & Hospitality	Any value	Any value	No approval needed
Sponsorships	Any value	Any value	No approval needed

- Must take reasonable and appropriate steps in relation to **Business Partners** to ensure their compliance with applicable Anti-Bribery and Corruption laws
- Must refer to relevant policies for activities, such as **Charitable Donations**, not covered by this Policy
- Must report any Bribery, Corruption, Fraud, illegal, unethical or unacceptable conduct that you know or suspect may violate this Policy and/or applicable laws, rules and regulations at the earliest possible opportunity. Failure to do so is a breach of this Policy and may be subject to disciplinary action (including potentially termination of employment).

This Policy is to be used in conjunction with the **Mubadala Group Code of Ethics** and any other relevant Mubadala Group or local policies.

Applicability & Consequences:

This Policy applies to the Mubadala Group and to **Mubadala Group Personnel**. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities.

Assets 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.

Your Responsibilities:

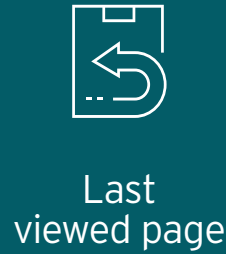
- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the **Mubadala Group Code of Ethics**, other Ethics & Compliance Policies, and any Corporate Unit/Business Unit or Asset policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy

Questions & Reporting Violations:

Report in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.

Failure to promptly report any known or suspected violations of this Policy to the Ethics & Compliance Office is itself a breach of this Policy and may result in disciplinary action (including potentially termination of employment).



POLICY REQUIREMENTS

You are prohibited from offering, providing, promising, receiving a Bribe and will not be penalized for refusing to pay or accept a Bribe.

You cannot offer or receive a Facilitating Payment or any other form of improper payment.

You should report instances of attempted or suspected **Bribery and Corruption** promptly to the Ethics & Compliance Office. Failure to do so is itself a breach of this Policy and may result in disciplinary action (including potentially termination of employment).

Subject to the requirements in this Policy, you may engage in legitimate business activities such as giving and/or receiving Gifts, Entertainment & Meals, Sponsored Travel & Hospitality and Sponsorships.

You should not threaten or retaliate against anyone who refuses to engage in activity prohibited by this Policy, or who raise concerns about possible wrongdoing under this Policy – even if we lose business or otherwise suffer a business disadvantage.

1. General Requirements

Any Gift, Entertainment & Meal, Sponsored Travel & Hospitality or Sponsorship:

- a. Must be directly related to Mubadala Group business, for a legitimate business purpose, of a value and nature that is customary in the particular industry and location, not lavish or extravagant, and otherwise appropriate and proportionate
- b. Must not be used as a tool to improperly influence or appear to influence you or anyone else or have the intention of improperly obtaining or retaining business or any business advantage
- c. Must not be construed or viewed reasonably as a Bribe
- d. Must not be received or offered at a time where it will

create an actual or perceived **Conflict of Interest**. For example, receiving a Gift from a bidder during a tender process that you are evaluating is prohibited

- e. Must not be received from or offered to a party who has a reputation for impropriety, unethical, or illegal conduct
- f. Must not include personal discounts, preferential stock options, or other benefits from suppliers, service providers, competitors, customers, or other third parties that are not available to the general public or to other Mubadala Group Personnel
- g. Must not violate any law, regulation, or applicable policy in place at the offeror's or recipient's organization. It is your responsibility to check
- h. Must not embarrass you or the Mubadala Group if any aspect of the exchange (including the value, nature, venue and identity of any fellow guests, etc.) were to be disclosed to the public
- i. Must involve the Ethics & Compliance Office when a decision is made to return or reject any Gift, Entertainment & Meal, Sponsored Travel & Hospitality or Sponsorship. The Ethics & Compliance Office will deal with the return to the offeror through appropriate channels
- j. Must be offered or received by you directly and not through any indirect means (for example, via a Related Person or another intermediary).

You must disclose if asked to speak at events or conferences, conduct lectures, or provide educational workshops, as these may attract attendance fees, Gifts, Entertainment and Meals etc. Participation in these events must also be notified to your Communications representative in accordance with the **Mubadala Group Communications Policy**.



Summary



Requirements



Policy Details

Blanket approvals are discouraged. If there is a strong business need for offering fixed Entertainment or Meals through a blanket approval you must request approval from the Ethics & Compliance Office.

When given, any Gift, Entertainment & Meal, Sponsored Travel & Hospitality or Sponsorship they must be accurately and timely recorded in the relevant books, records and accounts in accordance with applicable legal and accounting requirements. Your expense receipts must accurately reflect the date, value, nature, recipient(s), attendee(s), and venue.

Where applicable, Gifts, Entertainment & Meals, Sponsored Travel & Hospitality or Sponsorship must be pre-approved by your Business Leader and the Ethics & Compliance Office in accordance with this Policy.

2. Gifts

- Gifts must not consist of cash or a cash equivalent (e.g., vouchers, gift cards, etc.)
- No Gift (of any kind or value, even customary) may be offered or provided by Mubadala Group Personnel or the Mubadala Group to any Emirate of Abu Dhabi Government Entity and/or Abu Dhabi Government Official on a **Public Occasion**. No approvals will be provided for such Gifts
- Outside Public Occasions, during meetings and official visits, token Gifts may be provided to an Emirate of Abu Dhabi Government Entity and/or Abu Dhabi Government Official. The token Gifts must be branded (where possible), inexpensive, appropriate to the occasion, and pre-approved by the Ethics & Compliance Office
- Gifts must not consist of a Charitable Donation or donation to a political party
- Gifts - where possible - should incorporate an appropriate company logo to demonstrate the

business purpose of the Gift and limit transferability

- Corporate VIP Gifts must be obtained from the relevant Communications function and approved by the Ethics & Compliance Office
- If the value threshold below is met, you must obtain approval from your Business Leader and the Ethics & Compliance Office before purchasing, offering, or receiving a Gift. In cases of demonstrable emergency where pre-approval is not possible, you must seek and obtain approval as soon as possible after giving / receiving the Gift.

Pre-approval requirements (giving to / receiving from)			
	Government Official/Entity	Commercial Entity	Mubadala Group
Gifts	Any value	>= AED 550 (USD 150) per person/per event	No approval needed

3. Entertainment & Meals

- At least one representative from the offeror and recipient organization must be present and together at the Entertainment or Meal for the duration of the event
- When offering or providing Entertainment or a Meal, all costs must have been or will be, to the extent possible, paid for directly by the offeror, rather than advanced or reimbursed to the recipient
- Ensure that you follow your internal policies and guidelines for reimbursement of alcoholic beverages, if they are served during business meals
- Unless required by law, regulation or contract, we do not provide per diems or reimbursement to non-Mubadala Group Personnel. Additionally, you should not receive reimbursements or per diems from outside the Mubadala Group unless pre-approved by the Ethics & Compliance Office

- If the value threshold below is met, you must obtain approval from your Business Leader and the Ethics & Compliance Office before offering or receiving Entertainment or a Meal. In cases where preapproval is not possible, you must seek and obtain approval as soon as possible after the event

Pre-approval requirements (giving to / receiving from)			
	Government Official/Entity	Commercial Entity	Mubadala Group
Entertainment & Meals	Any value	>= AED 550 (USD 150) per person/per event	No approval needed

4. Sponsored Travel & Hospitality

- The trip must be directly related to a legitimate business purpose
- The duration must not exceed what is needed for the purpose of the trip, unless additional time is on your personal account
- The duration of the trip should be taken as official leave in the relevant attendance tracking system
- Expenses must be limited to those necessary to carry out the purpose of the trip
- Costs associated with the trip should be directly paid by the offeror to the third-party provider and not paid for or reimbursed to the recipient. In situations where this is not possible, company or entity accounts should be used for the payment of expenses. It is prohibited to reimburse expenses from personal accounts. All payments should be accounted for and invoices/receipts should be issued/received
- Regardless of value, you must obtain approval from your Business Leader and the Ethics & Compliance Office before offering or receiving any Sponsored



Travel & Hospitality of any amount. In cases where pre-approval is not possible, you must seek and obtain approval as soon as possible after the event

5. Sponsorships

- If you are approached by any party that invites the Mubadala Group to sponsor an event, direct that party to your Communications function, which manages Sponsorship requests
- Sponsorships must be aligned with business strategy and approved by your Business Leader, Communications function, and the Ethics & Compliance Office
- Sponsorships offered or given by the Mubadala Group should preferably be offered to organizations rather than to individuals
- All Sponsorships must be formalized in a legal agreement detailing the business benefit for the Mubadala Group in exchange for providing the Sponsorship. Legal & Governance must be involved to ensure that an appropriate agreement is used
- Each offer or receipt of Sponsorship must be preapproved, regardless of value, by your Business Leader, the Ethics & Compliance Office and the appropriate Communications function

6. Pre-approval process

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

- Follow your internal approval process before seeking pre-approval from the Ethics & Compliance Office
- Follow the instructions and complete the

appropriate pre-approval form. Approval forms are available on the Ethics & Compliance Office intranet at <https://ethics.mubadala.ae>.

In rare / emergency cases where preapproval is not possible, you must seek and obtain approval as soon as possible after the event

7. Other activities not covered by this Policy

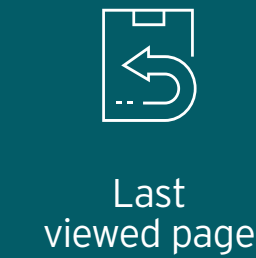
- Charitable Donations are managed and approved by Mubadala Group Communications
- Certain sectors or industries, deal with unique activities that require specific policies to manage situations that may also be covered by this Policy.

8. Business Partners

- Business Partners that violate applicable Anti-Bribery and Corruption laws can put the Mubadala Group at risk of reputational damage, fines, and penalties.
- It is therefore our duty to undertake the following:
 - a. Conduct appropriate risk-based **Due Diligence** on Business Partners and exercise appropriate, ongoing monitoring of them. Refer to the **Business Partner Due Diligence Policy** for further information and requirements
 - b. Include appropriate provisions in contracts with and/or obtain certifications from Business Partners that commit them to comply with applicable Anti-Bribery and Corruption laws
 - c. Conduct Anti-Bribery and Corruption training for or with a Business Partner, when appropriate
 - d. Provide the Business Partner with the **Business Partner Code of Conduct** and seek assurance that the Business Partner will comply



BUSINESS PARTNER DUE DILIGENCE POLICY



POLICY SUMMARY

This Policy sets out the minimum expectations for Business Partner Due Diligence with the aim of ensuring that we only do business with **Business Partners** who meet our standards in relation to ethics, integrity and compliance, and who have a shared commitment to abiding by applicable laws and regulations. Failure to comply with these requirements may lead to fines, loss of necessary operating authorizations, restrictions on government contracts, and other legal penalties. In addition, the poor conduct of a Business Partner may impact negatively on our reputation.

To manage these Business Partner-related ethical, compliance and legal risks, we must conduct appropriate, risk-based **Due Diligence**.

Due Diligence is the process undertaken to assess the level of risk posed by a potential Business Partner and involves gathering, analyzing, managing, and monitoring information about them. It includes checking the legitimacy and background of Business Partners before they commence a business relationship with the **Mubadala Group** and monitoring them throughout the course of that relationship.

Due Diligence risks are separate from commercial, operational, financial or other risks that are managed through other processes, e.g., supply chain and procurement or financial credit worthiness. Nonetheless, the Business Partner Due Diligence process may (and sometimes should) be incorporated into already existing processes and procedures established by a Corporate Unit/Business Unit or Asset.

In addition, **Anti-Money Laundering (AML)** and **Counter Terrorist Financing (CTF)** laws and regulations may require Due Diligence on customers to identify, mitigate and manage AML/CTF risks.

This Policy is to be used in conjunction with the Mubadala Group Code of Ethics and any other relevant Mubadala Group or local policies.

Applicability & Consequences:

This Policy applies to the Mubadala Group and to **Mubadala Group Personnel**. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities.

Assets 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**.

Your Responsibilities:

- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the **Mubadala Group Code of Ethics**, other Ethics & Compliance Policies, and any Corporate Unit/Business Unit or Asset policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy

Questions & Reporting Violations:

Refer in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.



Summary



Requirements



Policy Details



POLICY REQUIREMENTS

The steps below will help ensure that we select Business Partners that reflect our values and maintain our integrity and reputation:

- Implementation of a written process for engaging Business Partners
- Identification of Business Partners
- Assessment of commercial needs (not covered by this Policy)
- Risk-based documented Due Diligence
- Formal engagement with each Business Partner (e.g., a written contract)
- Monitoring and auditing of our relationship with each Business Partner
- Financial controls to ensure that payments are received from or made to the engaged Business Partner and that payments are earned and legitimate

We must also ensure that appropriate, risk-based Due Diligence is conducted. In operational terms, this means making appropriate inquiries to determine whether an existing or prospective Business Partner will meet our standards in relation to ethics and compliance, and that they have a shared commitment to abiding by applicable laws and regulations (e.g., ensuring the Business Partner is honest and will refrain from engaging in corruption and/or improper conduct).

You should not threaten or retaliate against anyone who refuses to engage in activity prohibited by this Policy, or who raise concerns about possible wrongdoing under this Policy - even if we lose business or otherwise suffer a business disadvantage.

1. Identifying Your Business Partners

The first step is for you to identify the potential Business Partner. For guidance, Business Partners

generally fall into one of the following categories:

- **Agent/Commercial Intermediary:** An individual or organization authorized to act for or on behalf of, or to otherwise represent, another organization in furtherance of its business interests. Agents may be categorized into the following two types: sales agents (e.g., those needed to win a contract) and process agents (e.g., those who help obtain visas, permits, licences etc.)
- **Advisor and other intermediary:** An individual or organization providing services and/or advice by representing an organization towards another person, business and/or **Government Official** (e.g., legal, tax, financial advisor or consultant)
- **Contractor:** A non-controlled individual or organization that provides goods or services to an organization under a contract. A subcontractor is an individual or organization that is hired by a contractor to perform a specific task as part of the overall project
- **Supplier/vendor:** An individual or organization that supplies products or services to another organization
- **Service provider:** An individual or organization that provides another organization with functional support (e.g., communications, logistics, storage, processing services)
- **Joint venture partner:** An individual or organization which has entered into a business agreement with another individual or organization (and possibly other parties) to establish a new business entity and to manage its assets
- **Consortium partner:** An individual or organization which is pooling its resources with another organization (and possibly other parties) for achieving a common goal. In a consortium, each participant retains its separate legal status
- **Customer:** The recipient of a purchased product, service, or idea



Summary



Requirements



Policy Details



2. Business Partner Justification

The process of justifying Business Partners is beyond the scope of this Policy. Nevertheless, a justification generally will assess, for example, whether a particular Business Partner fulfils a business need, is qualified, is not unnecessarily duplicative, and is financially sound. The **Relationship** or **Account Owner** must ensure the appointment of a Business Partner complies with any applicable Delegation of Authority, legal and procurement requirements. Once the commercial need for a Business Partner has been established, the Due Diligence process begins.

3. Risk Assessment

You must assess the level of risk posed by each Business Partner relationship. This risk assessment then establishes the appropriate level of Due Diligence that should be conducted such that you are comfortable that they will not present an unmitigated or unreasonable legal, commercial, or reputational risk.

4. Conducting Due Diligence

a. Application of Due Diligence

Once the level of risk has been determined, appropriate risk-based Due Diligence must be performed. This may be done using manual processes or procedures or by using automated systems and processes that are available. The Relationship or Account Owner is responsible for ensuring that appropriate risk-based Due Diligence is conducted and for managing the Due Diligence process.

Initial risk indicators to consider may, for illustration, include:

- Geographical location where services/products are being provided or where the Business Partner has its place of

business

- Industry in which the services are being provided
- Background and identity of Business Partner's beneficial owners and shareholders
- The Business Partner's connection or interaction with Government Officials or entities
- Compensation structure for payment (including proposed or actual spend)
- The process for selection of the Business Partner

b. Levels of Due Diligence

There are generally three levels of Due Diligence: Low, Medium, and High. The chart below describes each level of Due Diligence in very broad terms; each successive level includes the preceding steps:

Basic/Low	Medium	High
• Restricted Party screening • Basic company information collection • Internet and media research	• Company profile and history • Litigation and criminal records • Public records research	• Financial assessment • Interview information sources • Potential in-person site visits and/or interviews

For Low-risk Business Partners, basic information together with **Restricted Party** screening may be sufficient Due Diligence. Where a Business Partner is High-risk this does not automatically mean that we cannot engage with them. However, for High-risk Business Partners the greater the risk, the greater the level of scrutiny you should apply. In particular, you are required to:

- Be familiar with the nature of the Business Partner's activities
- Identify the source of or use of funds

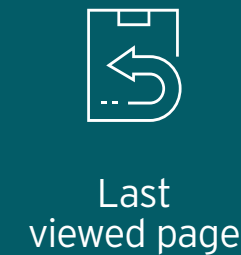
- Identify **PEPs** in a transaction or relationship
- Investigate and mitigate, where possible, red flags
- Request High-risk Business Partners to provide additional information to safeguard against **Money Laundering and Terrorist Financing**
- Know and verify the true identity of Business Partners using reliable and independent sources, documents, data or information
- Identify and verify the beneficial owners of Business Partners, including ownership and control structures

It is very important to factor in the time necessary to conduct appropriate Due Diligence. Lack of time is not an excuse for not doing so.

Higher levels of Due Diligence - known as enhanced Due Diligence - may be performed/managed by the Relationship or Account Owner or outsourced to a specialized Due Diligence service provider. We have Master Services Agreements in place with several enhanced Due Diligence service providers. Please contact the Ethics & Compliance Office for further information regarding the service providers and service levels for enhanced Due Diligence options. For any investment partner/investment target and for any Business Partner that goes to the Platform IC/Investment and Business Planning Committee/Investment Committee for approval, a Level 2 report is required in advance.

Business Partners whose responses to the Due Diligence Questionnaire indicate an elevated risk will be assigned a mandatory online Anti-Bribery & Corruption training as an additional requirement for the Due Diligence process.

Once Due Diligence is complete, an appropriate person (e.g., an appointed member of procurement



or other function, Legal & Governance or Ethics & Compliance) within the Corporate Unit/Business Unit or Asset should review the Due Diligence results, provide recommendations and/or conditions, and sign off on the Due Diligence. To maintain the integrity of the process and segregation of duties, Due Diligence should be approved by the due diligence analyst within the Ethics & Compliance Office, or any other individual who has been formally assigned the approver role by the Ethics & Compliance office.

If another Asset or Corporate Unit/Business Unit has conducted Due Diligence on a particular Business Partner, it is not necessary for Due Diligence to be repeated, provided the previous Due Diligence report or information is available, the Due Diligence already conducted is appropriate, relevant and risk-based for the subsequent relationship, and is no more than 12 months old.

c. Sanctions & Restricted Party screening

International sanctions are restrictions imposed by countries or international organizations, such as the United Nations, to influence the conduct of other countries or organizations. Sanctions may restrict business dealings within particular countries, or with particular persons, entities, or organizations. Sanctions risks should therefore be a key consideration as part of any assessment of business opportunities and Business Partners.

Restricted Party screening is intended to ensure that we know if our Business Partners are a Restricted Party. As a result, to ensure that transactions are performed legally and do not violate any applicable trade controls, sanctions, embargoes, or denied party restrictions, risk-based Restricted Party screening should be a key part of the Due Diligence performed on Business Partners, as identified above.

If you consider that a Business Partner, or anyone connected with them, is or may be a Restricted Party, you must seek Ethics & Compliance Office approval before proceeding further.

5. Red Flags

A red flag is something that indicates a potential risk and suggests that some form of additional or enhanced Due Diligence and/or risk mitigation (e.g., contract terms, representations, warranties, etc.) may be required. Whilst the presence of a red flag does not mean that we cannot engage with a Business Partner, you should ensure that you look out for red flags throughout the Due Diligence process.

Any red flags that are detected during the Due Diligence process should be mitigated or resolved prior to engaging with the Business Partner. Some potential red flags could include:

- The Business Partner appears to lack sufficient experience, capability, or qualified staff to perform the work for which it is being engaged (based upon the scope of work and business justification, years in business, staffing levels, sector, geography, etc.)
- The Business Partner has no physical presence in the country in which the work is to be performed
- The Business Partner is reluctant to provide requested information or references without a reasonable explanation, or the references provided raise a concern
- A Government Official - especially one with decision-making authority or influence - steered you to, recommended, or encouraged the use of the Business Partner
- The Business Partner is owned by a PEP, Government Official or a relative of a Government

Official

- The Business Partner claims that they can secure the deal because they know the right people or are able to “take care” of someone or red tape
- The Business Partner is a Restricted Party or has links to a Restricted Party
- The Business Partner, or a principal of the Business Partner, has been charged with, or convicted of, violations of anti-bribery, corruption, or Government procurement laws
- There are indirect or unusual payment or billing procedures, or the Business Partner’s fee is unusually high or exceeds the normal, arm’s length amount

However, this list is illustrative and is not intended to be exhaustive. Good judgement is also required at all times.

If/when you encounter a red flag, you should consider how to mitigate possible risks and whether additional Due Diligence is warranted. If it is not practical or feasible to mitigate the possible risk, you should determine whether the relationship with the Business Partner should be terminated or no longer be considered.

If you have questions about any red flag contact the Ethics & Compliance Office.

6. AML/CTF Due Diligence

Appropriate risk-based Due Diligence may also include assessing AML/CTF risks. You are strictly prohibited from engaging in and/or facilitating Money Laundering or Terrorist Financing. To that end, we cannot conduct business with an anonymous or fictitious company or with any Business Partner whose identity or business activities is unclear or unknown.

Risk-based AML/CTF Due Diligence on a Business Partner requires you to:



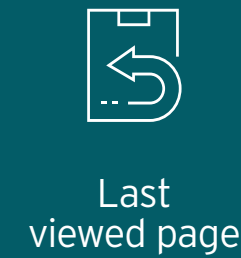
Summary



Requirements



Policy Details



- Know and verify the true identity of Business Partners using reliable and independent sources, documents, data or information
- Identify and verify the beneficial owners of Business Partners, including ownership and control structures
- The following is an illustrative (but not exhaustive) list of AML/CTF red flags:
- Methods or volumes of payment are not consistent with our payment policies or contract or are not ordinarily used in your business, e.g., payments with cash, money orders, traveller's cheques, or multiple instruments or payments from unrelated third parties
- Orders or purchases that are inconsistent with the Business Partner's trade or business (e.g., sophisticated integrated circuits purchased by a bakery)
- Payments to or from third parties or through countries that have no apparent connection with the transaction
- Payment instructions where there is a variation between the bank account name, the signatory, and the Business Partner legal entity
- Payments to or from countries considered to be tax havens or offshore jurisdictions or considered high risk for Money Laundering or Terrorist Financing
- Overpayment followed by directions to refund payment
- A Business Partner with beneficial owner(s) that cannot be identified or reluctance to provide information about the beneficial owner(s)

If you have any questions about AML/CTF Due Diligence, red flags, reporting requirements, risk mitigation, or any other AML/CTF matter please contact the Ethics & Compliance Office.

7. Formal Engagement

Upon successful completion of appropriate, risk-based

Due Diligence, the relationship with the Business Partner should be formalized. Ordinarily, this will be in the form of a contract or purchase order.

When formalizing the arrangement, the following should be considered:

- Scope of work and deliverables: Be specific and link payments to deliverables
- Formality: The Relationship or Account Owner should work closely with Legal & Governance to ensure that relevant clauses and appropriate provisions are included in the formal engagement, including references to our **Mubadala Group Code of Ethics** and our **Business Partner Code of Conduct**

8. Monitoring

The Due Diligence process does not end with formalizing the Business Partner relationship. Business Partners continue to present risk throughout the relationship. Therefore, it is important for the Relationship or Account Owner to continuously monitor the Business Partner relationship. As changes to the relationship occur, a new risk assessment and/or additional or repeat Due Diligence may be required.

Relationship changes that may trigger new or renewed Due Diligence may include a change in:

- Status of the geography: from a non-sanctioned to a sanctioned country or vice versa
- Size or scope of the relationship
- Type of relationship, e.g., from customer to supplier, from advisor to joint venture partner, etc.
- Ownership and/or control of the Business Partner
- Negative media reports

- Investigation announcement
- Restricted, denied, debarred, etc., party listing

9. Audit

If the Business Partner relationship includes audit rights, it is important for the Relationship or Account Owner to exercise those rights. An appropriate audit schedule for Business Partners should be established for routine audits and triggers should be implemented for non-routine audits (such triggers may include unusual payments received or requested; unusual orders; an unexplained increase or decrease in activity etc.).

10. Revalidation

The Corporate Unit/Business Unit Asset should revalidate any Business Partner no less frequently than:

- every 36 months from the date of initial review for Low risk Business Partners;
- 24 months for Medium risk Business Partners; and
- 12 months for High risk Business Partners, even if the contract term is longer, or sooner depending on other factors, e.g., risk, relationship, business practices, etc.

Recordkeeping

This Policy requires that the Due Diligence process is documented and that relevant records are retained for the period set forth in the relevant Corporate Unit/ Business Unit or Asset's record retention policy or practice.

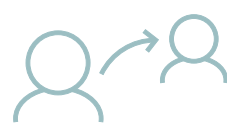




Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



PERSONAL TRADING POLICY



Summary



Requirements



Definitions



Policy Details





POLICY SUMMARY

This Policy sets out the requirements that are designed to assist you in recognizing market misconduct, understand how to avoid it, and know how and when to complete required disclosures related to your personal Securities trading activities, and how to report them to the **Ethics & Compliance Office**.

You must not trade, directly or indirectly, in publicly listed Securities while in possession of **Material Non-Public Information** about the company underlying those Securities. In addition, you cannot circumvent this Policy by trading Securities indirectly, for example, through a **Related Person**, partnership, trust, etc., or by directing or encouraging anyone to trade on your behalf.

You are permitted to trade in Securities in your personal capacity as long as you do not violate this Policy or any applicable law, rule or regulation. In addition, you are required to protect Material Non-Public Information related to Securities and must not engage in **Insider Trading or Securities Tipping**, or any other action in violation of applicable laws, rules or regulations.

When we receive Material Non-Public Information related to a Security, the Security will be classified as a **Restricted Security**, and those having access to such information will be classified as **Restricted Persons**. Material Non-Public Information may only be disclosed internally or externally in accordance with this Policy.

Material Non-Public Information received as part of your membership of a Board of a publicly listed company must not be disclosed to other **Mubadala Group Personnel** without pre-approval from the Ethics & Compliance Office. There may be personal trading disclosures and pre-approval requirements external to the **Mubadala Group** that apply to those who serve as directors of publicly listed companies, and it is your responsibility to understand and comply with those requirements.

This Policy is to be used in conjunction with the **Mubadala Group Code of Ethics** and any other relevant Mubadala Group or local policies.

Applicability & Consequences:

This Policy applies to the Mubadala Group and to Mubadala Group Personnel. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities.

Assets 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 review and approval.

Your Responsibilities:

- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the **Mubadala Group Code of Ethics**, other Ethics & Compliance Policies, and any Corporate Unit/ Business Unit or Asset policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy

Questions & Reporting Violations:

Refer in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.



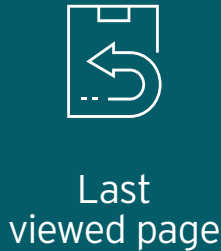
Summary



Requirements



Policy Details



POLICY REQUIREMENTS

1. What is market misconduct?

Market misconduct is a concept that encompasses unlawful behaviour in financial markets which in turn prevents full and proper market transparency.

For the purposes of this Policy, the term ‘market misconduct’ should be understood to include both Insider Trading and Securities Tipping, which are offences predicated on the abuse of Material Non-Public Information.

It is therefore important to understand how to identify and protect Material Non-Public Information.

2. Identifying Material Non-Public Information

Material Non-Public Information is information which:

- is of a precise nature;
- has not been made public;
- relates directly or indirectly to one or more publicly listed Securities; and
- would, if it were made public, be likely to have a significant effect on the price of those Securities.

In terms of identifying Material Non-Public Information:

- a. When is information precise? Information will be of a precise nature where it:
 - (i) indicates a set of circumstances that exists or may reasonably be expected to come into existence or an event that has occurred or may reasonably be expected to occur; and
 - (ii) is sufficiently specific to enable a conclusion to be drawn as to the possible effect of that set of circumstances or event on the price of financial

instruments or related instruments.

- b. When has information been made public? Whilst it will often be clear whether particular information is public, this is not always the case. Information about Securities is considered confidential until it has been fully absorbed by the marketplace. As a general rule, information should not be considered public until after the first full business day following the release of the information.
- c. When would information have a significant effect on price? Information which is likely to have a significant effect on price is information of a kind that a reasonable investor would be likely to use in deciding whether to buy, sell or hold a Security. For these purposes, information is likely to have a significant effect on price if there is a real (i.e., more-than-fanciful) prospect of the information having an effect on the price of Securities.

Although there is no figure or percentage change that can be set when determining the significance of an effect on price, a reasonable investor would be unlikely to take into account information having no, or merely a trivial, effect on price. The significance of the information in question will depend on a variety of factors (including recent developments and market sentiment).

Examples of information that would ordinarily be considered Material Non-Public Information include, but are not limited to, information related to:

- Earnings guidance and financial results
- Potential or actual gain or loss of a significant customer or supplier
- Pending or proposed mergers, acquisitions, restructurings, joint ventures, tender offers or changes in asset
- Plans to go into a new line of business or launch a new product



Summary



Requirements



Policy Details



- Changes in pricing policies
- Borrowing activities (other than in the ordinary course of business)
- Changes in dividend policy or capital structure (such as a stock split, changes to rights of Security holders, defaults, additional Security sales, etc.)
- Pending or threatened material litigation or regulatory action
- Change of external auditors
- Board or senior management changes
- Liquidity problems or anticipated credit rating changes
- Impending bankruptcy, receivership, or the existence of material cash flow problems
- Prospective significant trading by the Mubadala Group in a Security

Determinations of “materiality” are often very difficult to make, particularly when information comes from, or directly relates to, a third party (e.g., a key supplier or a competitor in a duopoly). You should not be making determinations of materiality independently. Contact the Ethics & Compliance Office and Legal if there is any question on materiality and allow them to make the determination.

3. Protecting Material Non-Public Information

Material Non-Public Information must only be accessible to those who need it for the proper fulfilment of their role. This means that no one should be given, or have access to Material Non-Public Information unless:

- it is necessary for them to have access to such information; and
- they have been made aware of and expressly acknowledged the confidentiality obligation which attaches to such information.

This is known as the Need to Know Principle and it applies to all Mubadala Group Personnel

a. General provisions

Material Non-Public Information must be protected at all times. You must not disclose Material Non-Public Information either internally or externally (including to any Related Person), except where authorized to do so by the **Deal Team Lead**.

Material Non-Public Information may be disclosed only to recipients who are within the **Deal Team** or who are third party advisors working on the matter and are contractually required to keep the information confidential. In the event you need to share Material Non-Public Information with Mubadala Group Personnel who are not included in the Deal Team, you must notify the Ethics & Compliance Office prior to disclosing the information.

When disclosing, sharing, or exchanging Material Non-Public Information, you must ensure that the information is marked with the appropriate confidentiality designation to alert the recipient of its sensitive nature and its disclosure restrictions.

If you receive requests to speak about or share Material Non-Public Information with the media or investment professionals, please contact the Ethics & Compliance Office in advance.

If you are not sure if information is Material Non-Public Information, or subject to disclosure restrictions, or if you believe you may have disclosed Material Non-Public Information in violation of this Policy, contact the Ethics & Compliance Office immediately.

b. Management & Committee Meetings

Prior to sharing Material Non-Public Information in meetings, whether internal or external, you must have previously notified the Deal Team Lead and Legal Counsel for the relevant Security and have jointly determined whether sharing the information will limit the ability of other Mubadala Group functions to conduct their duties. This requirement applies regardless of the nature of the meeting and includes, but is not limited to, meetings conducted for the

purpose of information sharing, decision making, or risk evaluation.

c. Board Memberships in Publicly Listed Companies

If you are a Director of a publicly listed company, you must understand and comply with all requirements and limitations applicable to you in your capacity as a Board member. You must take special precautions to segregate your Board and Mubadala Group employment roles, particularly when in possession of Material Non-Public Information. Material Non-Public Information received in a Board membership capacity may not be shared with other Mubadala Group Personnel without pre-approval from the Ethics & Compliance Office and the relevant publicly listed company. This requirement applies even if the Board membership was undertaken because the Mubadala Group is a shareholder of that publicly traded company.

4. Prohibition on Insider Trading & Securities Tipping

Trading in publicly listed Securities, while in possession of Material Non-Public Information concerning those Securities, is illegal.

You therefore must not trade, directly or indirectly, in Securities while in possession of Material Non-Public Information about the company underlying those Securities. This means that you must not:

- Buy, sell, or gift Securities of, or exercise stock options in, any company (including but not limited to our Assets) while aware of Material Non-Public Information about that company
- Give trading advice or disclose Material Non-Public Information (i.e., Securities Tipping) to anyone concerning any company while in possession of Material Non-Public Information about that company

This prohibition applies even if you might lose money by complying with the prohibition or if you have a personal financial emergency.

You may not circumvent this Policy by trading Securities



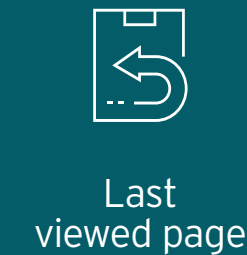
Summary



Requirements



Policy Details



indirectly, for example, through a Related Person or by directing anyone to trade on your behalf.

Transactions will be scrutinized after the event, with the benefit of hindsight. As a practical matter, before engaging in any transaction, you and your Related Persons should carefully consider how regulators, the media, and the public might view the transaction.

You should not threaten or retaliate against anyone who refuses to engage in activity prohibited by this Policy, or who raises concerns about possible wrongdoing under this Policy – even if we lose business or otherwise suffer a business disadvantage.

If you are not sure whether information is Material Non-Public Information and you want to trade, or if you believe that you may have traded while aware of Material Non-Public Information, contact the Ethics & Compliance Office immediately.

5. Classification of Restricted Securities

When we receive Material Non-Public Information related to a Security in the course of business, the Security in question will be classified as a Restricted Security. If you receive, or are anticipating receiving, such information on a regular or ad hoc basis in carrying out your responsibilities on behalf of the Mubadala Group, you will be classified as a Restricted Person and will be provided with access to a list of Restricted Securities applicable to you.

When all relevant information is publicly announced or is otherwise no longer considered Material Non-Public Information by Legal, that specific Security is no longer considered a Restricted Security and will be removed from the Restricted Securities List. At that point, associated Restricted Persons will no longer be restricted from trading in that Security.

If you receive Material Non-Public Information in the ordinary course of your Mubadala Group duties and you believe that the Ethics & Compliance Office is not aware, you are required to notify the Ethics & Compliance Office immediately, and you

must not discuss or disseminate the information further until further direction is received.

6. Requirements Applicable to Restricted Persons

You will receive a notification from the Ethics & Compliance Office informing you when you have been identified as a Restricted Person. The notification will detail your obligations and requirements, which will include at a minimum:

- **Disclosure of Restricted Securities:** You are required to disclose your personal holdings of any Restricted Securities. To disclose your holdings, you must complete the Restricted Securities Holdings Disclosure Form, which is available on the Ethics & Compliance Office intranet and submit the form to the Ethics & Compliance Office.
- **Trading in Restricted Securities:** You must not trade in any Restricted Security. In addition, you must always check that your Restricted Securities List is up-to-date before engaging in any Securities trading. This prohibition applies even if you believe that you are not in possession of Material Non-Public Information related to the Restricted Security you wish to trade. In extenuating circumstances, the Ethics & Compliance Office may waive the trading restriction but only for certain sell trades subject to pre-approval. To seek pre-approval to sell a Restricted Security, you must complete the Restricted Security Trade Request, which is available on the Ethics & Compliance Office intranet and submit the form to the Ethics & Compliance Office.

Even if a particular Security is not included on your Restricted Securities List, you are still prohibited from trading in any Security while in possession of Material Non-Public Information, and you must adhere at all times to the general obligations under this Policy and applicable laws, rules and regulations.

7. Disclosures & Holding Period

a. Personal Trading in Non-Restricted Securities

You are permitted to trade in Securities in your personal

capacity as long as you do not violate this Policy or any applicable law, rule or regulation.

Unless otherwise communicated to you, you may trade in Securities held by the Mubadala Group, provided they are not on your Personal Restricted Securities List and you are not in possession of any Material Non-Public Information related to those Securities.

b. Disclosure of Personal Trading

Certain Mubadala Group Personnel who regularly deal with publicly listed Securities as part of their Mubadala Group responsibilities will be required to disclose to the Ethics & Compliance Office, on a periodic basis, their personal transactions in Securities. The Ethics & Compliance Office will conduct periodic targeted reviews of such disclosures and may request from Mubadala Group Personnel copies of their brokerage account statements to verify the accuracy of reporting. If you are subject to this requirement, you will be notified and provided with further guidance. Non- Reportable Securities are not subject to disclosures and/or periodic targeted reviews.

If you are involved in a proposed Securities transaction on behalf of the Mubadala Group and in your personal capacity you have existing holdings in those Securities, you must complete the Personal Holdings Disclosure Form.

c. Other External Requirements

Trading in Securities may trigger additional disclosure or pre-approval requirements that are external to the Mubadala Group. It is your responsibility to find out what legal and regulatory requirements may apply to any Securities transaction you contemplate.

d. 60 Day Holding Period

Mubadala Group Personnel who purchase a Security, must hold that Security for at least 60 consecutive calendar days after the most recent purchase of the Security.



Summary



Requirements



Policy Details



DATA PRIVACY POLICY



Summary



Requirements

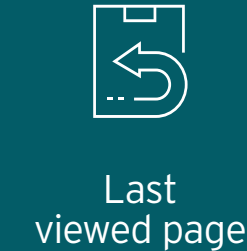


Definitions



Policy Details





POLICY SUMMARY

We are a global company with presence across many industries and territories. Each country and industry may have its own laws and regulations for data protection and **Processing**. Many of these laws and regulations protect information relating to **Persons** and restrict accessing **Personal Data**, sharing Personal Data with other **Mubadala Group Assets, Business Partners** or third parties, and/or transferring Personal Data across geographic borders.

This Policy sets minimum expectations to ensure that we adopt good practices and conduct our business in a compliant manner.

We need to ensure that data protection requirements are in place and met. This Policy sets out eight basic principles that must be adhered to when Processing Personal Data:

- Personal Data must be processed fairly, lawfully and transparently
- Personal Data must be obtained for lawful purposes and must not be processed in a manner incompatible with those purposes
- Personal Data must be adequate, relevant and not excessive in relation to the purposes for which it is being processed
- Personal Data must be accurate and kept up to date
- Appropriate technical and organizational measures must be taken against unauthorized or unlawful Processing of Personal Data, as well as against accidental loss, destruction of or damage to that data
- Personal Data must not be kept for longer than is necessary
- Personal Data must be processed in accordance with the rights of **Data Subjects**
- Personal Data must not be transferred outside the country in which it was collected unless the country to which it will be transferred is deemed to provide an adequate level of protection or the transfer is conducted subject to certain appropriate technical and

organisational safeguards (please contact your **Data Protection Lead (DPL)**, Legal & Governance or the **Ethics & Compliance Office** for a list of countries deemed to have adequate levels of protection and for guidance on what safeguards (if any) should be implemented for a proposed cross-border transfer of Personal Data)

In many countries, data protection laws protect individuals from abusive Processing, transferring and sharing of Personal Data. Violations of relevant data protection laws and/or employment laws may lead to legal proceedings and claims for damages against the violator (whether the violator is a company or individual).

You should not threaten or retaliate against anyone who refuses to engage in activity prohibited by this Policy, or who raise concerns about possible wrongdoing under this Policy – even if we lose business or otherwise suffer a business disadvantage.

Applicability & Consequences:

This Policy applies to the Mubadala Group and to **Mubadala Group Personnel**. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities.

Assets 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.

Questions & Reporting Violations:

Refer in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.

Your Responsibilities:

- Follow applicable laws and regulations
- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the **Mubadala Group Code of Ethics**, other Ethics & Compliance Policies, and any Corporate Unit/ Business Unit or Asset policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy
- Refer in good faith any questions, concerns, or any known or suspected violations of this Policy, including any queries, complaints or requests raised by a Data Subject to the Ethics & Compliance Office through the Contact Us section available refer to the contact us icon above.
- Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.
- policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy



Summary



Requirements



Policy Details

POLICY REQUIREMENTS

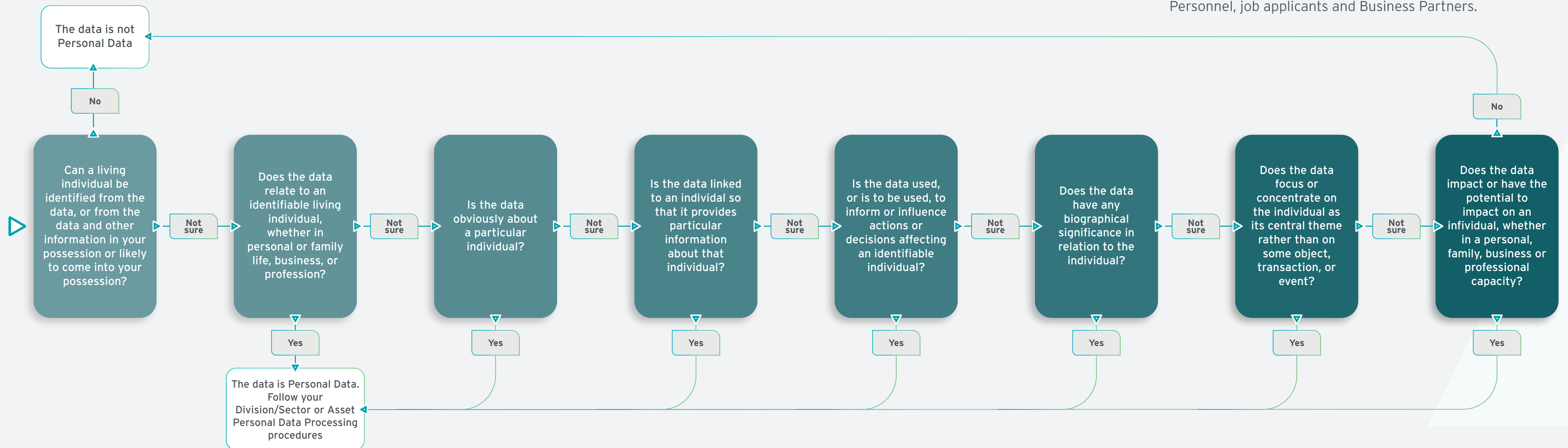
1. Personal Data

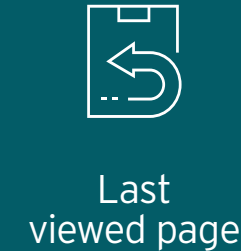
Personal Data is broadly defined as information that relates to an identified or identifiable Person (i.e., the Data Subject). There are different ways in which a Person may be identifiable. A Person's name is obvious Personal Data. A Person may also be identifiable from other information that may be used to reference another source, such as physical characteristics, social insurance number, address, employee ID number, e-mail address, etc., and also expressions of opinion about that Person. Personal Data remains subject to data protection laws even if it is publicly available, e.g., telephone number, e-mail address, etc.

In some countries, some types of Personal Data are classified as **Sensitive Personal Data** which is often given more protection. Sensitive Personal Data or **Special Category Data** may include (but is not limited to) race, ethnicity or national origin, political opinions or associations, union membership, marital status, health-related information, and criminal history.

We all have a responsibility for applying appropriate security measures for Personal Data, including Sensitive Personal Data or Special Category Data acquired from current or former Mubadala Group Personnel, job applicants and Business Partners.

The flowchart below illustrates how to determine whether information is Personal Data:





2. Principles for Processing Personal Data

- a. Mubadala Group Assets control, possess and process Personal Data relating to a variety of Persons, including current or former Mubadala Group Personnel, job applicants and Business Partners, often as a **Data Controller** of that Personal Data.
- b. In order to comply with legal requirements, we must process and protect Personal Data in a manner consistent with good practices and applicable law and we are responsible for and must be able to demonstrate compliance with the eight basic principles of data protection adopted under this Policy.
- c. Local law may permit deviation, exception or exemption from a principle under particular circumstances. Consult with the Ethics & Compliance Office prior to doing so, even if a deviation, exception or exemption is permitted by local law.

3. Principles of Data Protection

- a. **Fair and Lawful Processing:** Personal Data should be processed fairly, transparently (to the Data Subject), and in accordance with the law. To create transparency, Data Controllers are required to provide concise, accessible, clear, and plain information to Data Subjects including the identity and contact details of the Data Controller, purpose(s) of Processing, and the identity of anyone to whom the data may be disclosed or transferred. Local law may require additional information to be included in a Privacy Notice. A Data Controller may also be required by law to obtain consent from a Data Subject prior to Processing Personal Data.
- b. **Restriction to a Specific Purpose:** Personal Data should be collected only for specified and lawful purposes which are reasonably necessary to achieve our legitimate business-related interests. Personal Data

should not be processed in a manner incompatible with those purposes. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before carrying out any new Processing and give their consent (except in certain circumstances where a legal exemption from this obligation applies or their consent is not required under applicable laws and an alternative lawful basis applies). Purposes for Processing data always should be business-related, legitimate, and clear.

- c. **Relevance:** Personal Data must be adequate, relevant, and not excessive in relation to the purposes for which it is processed. This means Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Any Personal Data which is not necessary for that purpose should not be collected in the first place.
- d. **Accurate and Up-to-Date:** Personal Data should be accurate and updated when necessary. Suitable steps must be taken to ensure that inaccurate or incomplete data is deleted or corrected. Inaccurate or out-of-date Personal Data should be destroyed or erased from all Mubadala Group systems. This applies to paper records as well.
- e. **Technical and Organizational Security:** Appropriate technical and organizational security measures must be taken to prevent unauthorized or unlawful Processing and accidental loss, destruction, or damage to Personal Data. Access to Personal Data must be appropriate for the type and scope of the individual who will have access and on as-needed basis only. Your IT function should provide support for securing Personal Data and for **Anonymization** and **Pseudonymization** to ensure that data is kept confidential and secure. You must not disclose any Personal Data to a third party unless one or more of the following apply, and in the event that the recipient is in another jurisdiction, the disclosure complies with

cross-border transfer requirements under applicable law:

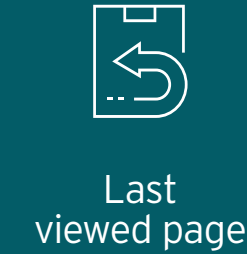
- i. Either the Data Subject has been informed in a Privacy Notice that their Personal Data may be disclosed to such parties and the purpose for which it is being disclosed, or the disclosure takes place in the course of conducting legitimate business activities and the Data Subject would expect their Personal Data to be used for this purpose
- ii. The disclosure is made with the consent of the Data Subject to whom the Personal Data relates. If you are disclosing Sensitive Personal Data, you must obtain the prior written consent of the Data Subject before you can disclose
- iii. The disclosure will be to an organization and/or individual entitled to receive the Personal Data, for example, to the police where the information is necessary to prevent or detect crime
- iv. The disclosure is made in order to comply with legal obligations placed on the Mubadala Group or to comply with a court order
- v. The disclosure is made in the course of legal proceedings
- f. **Data Retention:** Personal Data should not be retained longer than necessary (for example, only the time required to fulfill the purpose for which it was collected). Personal Data that is no longer required must be deleted and/or disposed of in a secure way that protects the interests of the Data Subject.
- g. **Rights of Data Subjects:** Depending on applicable law, Data Subjects are granted various rights under data protection laws. The key Data Subject rights, and the actions you need to take when those rights are exercised, are as follows:
 - i. The right to ask to see and access what Personal Data (and other supplementary information) we hold about them or other individuals and how we use their

Personal Data. Please refer any requests (whether made verbally or in writing) received from employees, former employees and potential recruits to Human Capital and written requests from any other individuals (for example from Business Partners) to the Ethics & Compliance Office immediately, as we may only have up to 30 days in which to respond to such requests. In cases where a Data Protection Lead (DPL) is appointed, the Data Protection Lead (DPL) must be informed.

Sometimes requests for Personal Data may be made verbally over the telephone - in which case you should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Ask the caller to put their request in writing if you are not sure about the caller's identity and where their identity cannot be checked
- Refer to the Ethics & Compliance Office for assistance in difficult situations. No one should be bullied or forced into disclosing Personal Data.
- ii. The right to require us to rectify any Personal Data which is inaccurate (made verbally or in writing). For example, if you are requested to change an address of a customer, client or supplier etc., you should make those changes immediately. If inaccurate Personal Data about a Data Subject has been passed on to a third party, it may also be necessary to correct the third party's data, depending on the nature of the data and whether the third party is still likely to be using it. If the Personal Data is of a more serious nature, keep a record of the change made and circumstances in which it was made and if you feel it is necessary, talk to the Ethics & Compliance Office about it.
- iii. The right to restrict Processing of their Personal Data where applicable, including if this has caused, or is likely to cause, damage or distress or the Data Subject contests the accuracy of the Personal Data we hold





about them, verbally or in writing. Please contact the Ethics & Compliance Office if you receive a request to prevent Processing.

- iv. The right to ask for the logic involved in any automated decision taken without human input (i.e. by a computer). Also, the right not to be subject to a decision based solely on automated means, if the decision produces legal effects concerning the Data Subject or significantly affecting them. In such cases, please contact the Ethics & Compliance Office.
- v. The right to prevent us from sending unsolicited marketing materials to them and, where applicable, object to our processing of their Personal Data, following an objection request made verbally or in writing. Depending on the type of unsolicited marketing, intended recipients may have a right to either opt-in or opt-out. Please contact the Ethics & Compliance Office if you intend to send any unsolicited marketing to named individuals or you receive an objection request from a Data Subject.
- vi. The right to erase Personal Data, where applicable, following a request for erasure made verbally or in writing.
- vii. The right to receive, where applicable, following a request made verbally or in writing, Personal Data provided to us as a Data Controller, in a structured, commonly used and machine readable format and the right to request that this Personal Data is transmitted directly to another Data Controller. Please contact the Ethics & Compliance Office if you receive a data portability request.

h. Data Transfer: Personal Data may only be transferred to another party (whether related or unrelated) or third party if there is a legitimate business purpose and the other party has data protection measures at least comparable to those set out in this Policy or as required by applicable law or regulation. In the event that the proposed recipient is in another jurisdiction, any transfer outside the geographical location in

which Personal Data was collected should be in compliance with cross-border transfer requirements under applicable law and pre-approved by the Ethics & Compliance Office to ensure the appropriate level of protection and compliance with applicable law.

3. Data Processing Legitimacy

Personal Data should be processed only for specified, clear, and legitimate purposes. Processing Personal Data is permissible if the intended Processing is:

- Performed with the valid consent (when required) of, or after proper notification to, the Data Subject (examples are available from the Ethics & Compliance Office)
- Necessary for the purpose of establishing a contractual relationship or similar relationship of trust with the Data Subject
- Necessary to safeguard justified interests of the business. It is important to note that this condition only applies if the Processing does not adversely affect the Data Subject concerned. If there is a serious mismatch of competing interests between the business and the Data Subject, the Data Subject's interests will have priority over business interests. If you are unsure whether there are competing interests, please contact the Ethics & Compliance Office
- Permitted or agreed by applicable local law and regulations
- Necessary for compliance with legal obligations
- Required to protect the life, health, or safety of the Data Subject

When processing Sensitive Personal Data, additional conditions required by applicable law must also be met. Please contact the Ethics & Compliance Office if you are unsure whether Personal Data is Sensitive Personal Data and for guidance in relation to these conditions.

4. Consents

Where required by law, or where an alternative lawful basis is not available, a Data Subject should give consent before any Processing, sharing, or transferring of their Personal Data. To be effective, consent must be valid in accordance with the requirements of applicable law. In particular, consent must be informed and specific, which means that the Data Subject must know and understand why the Personal Data is being processed, shared or transferred, and unambiguous, which means that the Data Subject must provide a clear affirmative signal. In addition, consent must be given freely and voluntarily in order to be valid, which means that Data Subjects must be able to refuse to consent without detriment. If you are unsure whether consent is valid or whether it would be more appropriate to rely on an alternative lawful basis, please contact the Ethics & Compliance Office. Consent may be given in written, electronic, or verbal form. Verbal consent should be noted in a record for future reference. Where prior consent is required, the purpose of the Processing may only be changed with the consent of the Data Subject or to the extent permitted by law. In some countries, Data Subjects must be informed about their right to withdraw consent and previously given consent may be withdrawn at any time, and the Data Controller must be able to demonstrate that it has acted on the request.

5. The Data Subject's Access Right and Request

We should allow Data Subjects reasonable access to Personal Data during normal working hours and upon reasonable request and will allow a Data Subject to update and/or correct inaccurate information. The Data Protection Lead shall establish a method to enable the Data Subject rights of access, removal, or rectification where appropriate and in compliance with Mubadala Group policies and procedures.



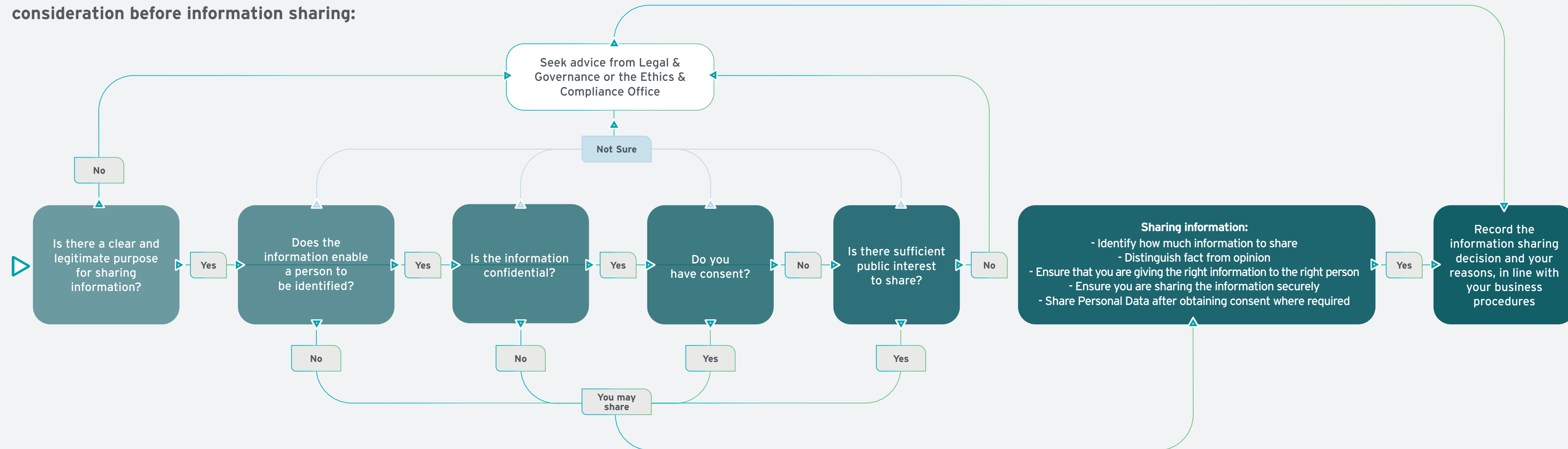
6. Data Sharing

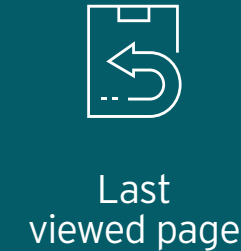
For some business processes, it may be necessary (e.g., legal obligation) or desirable (e.g., practicality) to share Personal Data outside the organization that possesses it. Before sharing or transferring Personal Data, we should consider if transmitting Personal Data (even if to related Mubadala Group entities) is necessary, appropriate, legitimate, and compatible with the purpose(s) for which it was obtained, or is in conflict with any interest of the Data Subject. The recipient must guarantee an adequate level of data protection in line with this Policy and applicable law and be bound by contract to process Personal Data only for specified, legal purposes. Set out below are some

key questions for consideration before sharing Personal Data:

In certain circumstances it may also be necessary for Personal Data originating in one country to be shared or made available or accessible in or to a different country. In many countries, such as the United Kingdom, the European Union and the DIFC and ADGM Free Zones, applicable data protection laws may restrict these cross-border personal data transfers. In addition to the above-referenced key considerations when transferring Personal Data outside of the organization, Personal Data must not be transferred outside the country in which it was collected unless one of the following conditions applies:

The flowchart below sets out some key questions for consideration before information sharing:





- The country to which the Personal Data will be transferred ensures an adequate level of protection for the Data Subject's rights and freedoms.
- The Data Subject provides specific, informed and express consent for the transfer.
- §The Ethics & Compliance Office, Legal & Governance or DPL (as applicable) concludes that the transfer complies with all relevant cross-border transfer restrictions, including any appropriate safeguards that must be implemented, and approves the transfer in writing.

7. Data Protection Lead (DPL) and General Provisions

Clause 7.a. is applicable where we are required by law and/or regulation to appoint a Data Protection Lead (DPL). If you are not certain about such a requirement, please contact the Ethics & Compliance Office for clarification and guidance. Where there is a need for a DPL, the following provisions apply, to the extent that the law and/or regulation does not provide otherwise:

- Leadership** will appoint one person or a team of persons to be its DPL. The DPL need not be a full-time role or new position within the organization. The business may assess and decide, according to its needs, whether the DPL should be a dedicated responsibility or an additional responsibility of an existing role in the business. The responsibilities of a DPL may include, but are not limited to, the following:
 - Identify the Personal Data controlled, requested, acquired, processed, and/or maintained by the business and alert the business to any risks that might arise with regard to data privacy
 - Develop processes and procedures for handling Personal Data that are in compliance with this Policy and local law and are suitable to business needs
 - Support the implementation of the data

privacy program, demonstrate commitment to accountability, and implement mechanisms to ensure responsible decision-making about the protection of Personal Data and adoption of internal practices consistent with the law and this Policy

- Support mechanisms and procedures for individuals to report misuses or inappropriate disclosure of Personal Data and support appropriate remediation and disciplinary actions
 - Consult with the Ethics & Compliance Office and information security team before establishing or updating any system, process, or procedure to collect, use, disclose, or transmit Personal Data
 - Notify the Ethics & Compliance Office of any data breach to comply with relevant data protection regulations and legislation. In case of data breach contact cybersecurity@mubadala.ae, digitalcare@mubadala.ae or edm@mubadala.ae.
 - Monitor the proper use of Personal Data Processing, transferring, sharing, and disposing of Personal Data in accordance with applicable data privacy regulations and this Policy
- Human Capital departments are custodians of the majority of Personal Data. Such Personal Data is not limited to employee data, but includes potential new candidates' Personal Data. Personal Data collected for recruitment must be limited to the information necessary to evaluate the suitability of a candidate and career potential, and to perform any necessary security or other vetting. Human Capital should follow their own processes and procedures before Processing Personal Data, in alignment with this Policy.
 - Human Capital should inform employees and candidates about the purposes for which Personal Data will be Processed, the type of Personal Data stored, the parties with which Personal Data is regularly shared

(including Government bodies), and the purpose of such sharing and Processing. It is sufficient in this regard that employees are informed about Processing by means of a Human Capital policy (or similar method). Local laws take precedence over this Policy; where such laws impose more stringent requirements, it is essential to follow such local laws.

- Sometimes we may use an external party to assist and support Processing activities. The external party must provide necessary security measures and take reasonable steps to ensure compliance with this Policy and applicable laws and regulations. A written contract shall require a third party processor to comply with data privacy and security requirements and will require notification to the Ethics & Compliance Office, if a breach occurs.
- In certain jurisdictions, we may use Pseudonymization to protect Personal Data. Pseudonymization is not the same as **Anonymization** and in certain jurisdictions different requirements apply to each technique. In either case, Anonymization and Pseudonymization techniques must be used fairly and in accordance with applicable law so please liaise with the Ethics & Compliance Office, if you intend to Anonymize or Pseudonymize Personal Data.
- You should monitor and conduct checks on the Processing of Personal Data by any third party, especially in respect of security measures to ensure compliance with this Policy and contractual commitments.



Summary

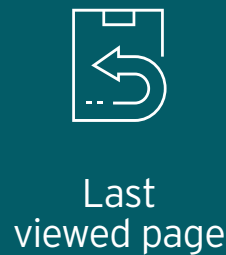


Requirements



Policy Details

E&C ARTIFICIAL INTELLIGENCE POLICY



POLICY SUMMARY

At **Mubadala Investment Company (Mubadala)**, we are committed to leveraging the power of **Artificial Intelligence (AI)** to drive innovation, enhance efficiency, and do better work. Our AI strategy revolves around three main pillars: investing better, working smarter, and accelerating impact, which reshape investment practices to deliver superior results. While recognizing the potential risks of AI, we seek to balance these with the opportunities AI presents. As part of Abu Dhabi's broader digital strategy, Mubadala seeks to position the emirate of Abu Dhabi as a global leader in AI-driven governance and innovation, contributing to sustainable economic growth. We will prioritize responsible use, data security, and ethical considerations as we embrace AI technologies. This Policy outlines the goals, use, and guidelines around using AI tools in compliance with our Code of Ethics and as an extension of our company values.

Effective AI governance is crucial for ensuring that our use of AI aligns with our ethical standards, regulatory requirements, and strategic objectives. By implementing robust governance practices, we can mitigate risks, enhance transparency, and foster trust among our stakeholders. This commitment to responsible AI use not only safeguards our reputation but also drives innovation and operational excellence, positioning Mubadala as a leader in the ethical and effective deployment of AI technologies.

This Policy covers all **Artificial Intelligence** technologies used within Mubadala, including:

- Large language models (LLMs) and Generative AI;
- Investment decision support systems; and
- Compliance and risk management AI systems,
- (together, **AI Tools**).

This Policy applies to AI Tools developed internally, procured from vendors, or accessed through third-party services. It should be read in conjunction with the following existing Mubadala policies and codes: **Mubadala AI Policy, Acceptable IT Usage, Data Security Standard, Data Governance Policy, Code of Ethics** and **Risk Management Policy**.

The purpose of this Policy is to:

- Establish clear guidelines for responsible AI use across Mubadala Group;
- Define governance structures for AI oversight and accountability;
- Ensure regulatory compliance and risk management in AI implementation;
- Promote ethical AI practices; and
- Outline training requirements for employees at all levels.

1.1 Applicability & Consequences

This Policy applies to Mubadala and to all **Mubadala Group Personnel**. Those who fail to uphold the provisions and the spirit of this Policy put themselves, their colleagues, and Mubadala at risk of fines, penalties, civil and/or criminal liability, and reputational damage. They may also be personally subject to disciplinary action, up to and including loss of employment.

The legal and regulatory landscape in this area is constantly evolving. This Policy will be reviewed periodically to ensure: (i) alignment with evolving regulatory requirements; (ii) incorporation of emerging best practices; and (iii) ongoing effectiveness in managing AI risks and opportunities, including in light of new AI capabilities and use cases. We reserve the right, at our sole discretion, to disclose information about violations of law to relevant authorities. Portfolio Companies may establish standards that are stricter than this Policy. Any proposed exceptions to or deviations from this Policy must be submitted to the Mubadala Ethics & Compliance Office.

1.2 Your Responsibilities

- Uphold our commitment to always do what is right
- Demonstrate ethics, integrity, and accountability at all times and expect the same from others
- Understand and comply with the requirements of this Policy, the Mubadala Group Code of Ethics, other Ethics & Compliance Policies, and any Business Platform policies or procedures in relation to this Policy
- Provide appropriate resources and support to ensure the successful implementation of this Policy
- Complete assigned training relating to this Policy

1.3 Questions & Reporting violations

Promptly report in good faith any questions, concerns, or any known or suspected violations of this Policy to the Ethics & Compliance Office through the Contact Us section (refer to the icon above).

Retaliation for good-faith reporting is not tolerated. Those who engage in retaliatory conduct will be subject to disciplinary action.

Failure to promptly report any known or suspected violations of this Policy to the Ethics & Compliance Office is itself a breach of this Policy and may result in disciplinary action.



Summary



Requirements



Policy Details



POLICY REQUIREMENTS

2.1 Mubadala Guiding Principles relating to E&C Artificial Intelligence Policy

Mubadala adheres to the following principles in all AI development, procurement, and deployment:

- (i) **Excellence and Innovation:** Mubadala supports innovation to generate diverse ideas and solutions, improving overall engagement, enhance efficiency, and do better work. We strive for innovation and excellence in our AI initiatives, fostering a culture of continuous improvement and adapting to new technologies.
- (ii) **Ethical Integrity:** We develop and deploy AI Tools that align with Mubadala's Values and commit to using AI in ways that benefit our stakeholders.
- (iii) **Human-Centric Design:** Our use of AI is intended to prioritize human values and ensure AI serves and enhances human capabilities. We maintain appropriate human oversight of AI Tools, including for consequential investment decisions. AI Tools augment rather than replace human judgement in client-facing activities and material investment decisions.
- (iv) **Fairness and Non-Discrimination:** We implement processes to identify and mitigate biases in AI Tools and regularly audit AI models to mitigate any risk that they perpetuate or amplify existing biases. We ensure AI Tools are designed and deployed in a manner that seeks to promote equal opportunity and not to discriminate against any individual or group based on factors like race, gender, or age and that seeks to ensure that algorithms treat everyone equitably, including by using diverse and representative data sets to train AI models.
- (v) **Transparency and Explainability:** We develop AI Tools that seek to provide clear and understandable explanations for their decisions and outputs, so that users can comprehend how and why decisions are made. Mubadala maintains open lines of communication with stakeholders about the use of AI, including its benefits, risks, and limitations. As part of this, we maintain comprehensive documentation relating to the AI Tools we use, including their development processes, data sources, and decision-making criteria. Where we leverage third party AI assets, we expect our AI suppliers to provide us with the necessary information to meet these standards.
- (vi) **Governance and Accountability:** Mubadala will guide, align, and

oversee the development, acquisition, and use of AI Tools in line with this Policy and Mubadala's Values and purpose. Mubadala uses a risk-based framework to manage AI, ensuring that governance requirements for each AI system and use case are proportional to the associated risks.

- (vii) **Data Privacy and Security:** Respecting individual privacy rights through responsible data governance and ensuring sensitive and lawful handling of data collection, use, storage, and sharing are key to Mubadala's responsible use of AI. Personal Data (as defined in the **Data Privacy Policy**), must only be used with AI Tools where necessary and proportionate and otherwise in a manner consistent with the Data Privacy Policy and this Policy. You must not, without pre-approval, input any material non-public information, highly confidential information or software code into AI Tools. The use of approved AI Tools must also adhere to [Mubadala's Acceptable IT Usage policy](#).
- (viii) **Compliance and Testing:** AI Tools will be evaluated, where appropriate, with a view to ensuring they produce accurate, reliable, and consistent outputs. Reasonable steps will be taken to implement appropriate measures, including human oversight or technical safeguards, to align AI deployment with Mubadala's principles, policies, and procedures. Certain data sets may be assessed for quality, timeliness, completeness, and representativeness with a view to ensuring AI Tools function as intended. Where appropriate, AI Tools or their uses will be reviewed for compliance with relevant laws and regulations.
- (ix) **Continuous Monitoring and Improvement:** AI Tools will be continuously monitored for performance, accuracy, and ethical compliance. It may be necessary to monitor sensitive data inputs, the performance of AI Tools, and their use by employees to ensure the systems are operating as intended, to prevent model drift (the phenomenon where the performance of an AI model degrades over time due to changes in the underlying data or environment, necessitating regular monitoring and updates), or to prevent misuse.
- (x) **Accuracy and Fact Checking:** Generative AI can produce results that are inaccurate, incomplete, or misleading (often referred to as "hallucinations"). Whenever you use AI Tools you must verify the facts, data, and statistics generated by AI to ensure accuracy before publication or distribution.



Summary



Requirements



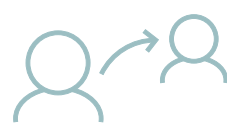
Policy Details



Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



DEFINITIONS



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

54

/ 60





Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

Advisory Board: A body that advises the Board of Directors and/or management of a company but does not have any fiduciary responsibilities or the authority to vote on corporate matters; examples include business, editorial, technical, and scientific Advisory Boards.

Anonymization: Elimination of all identifying elements from Personal Data; no element may be left that could serve to re-identify the Person. Where information has been successfully anonymized, it is no longer Personal Data.

Anti-Money Laundering (AML): A set of procedures, laws, or regulations designed to stop the practice of legitimizing (i.e., laundering) funds obtained by illegal means.

Artificial Intelligence (AI): Machine-based systems that use input data to infer how to generate outputs (such as predictions, content, recommendations, or decisions) in response to explicit or implicit objectives and reach conclusions through reasoning and self-correction to improve analysis. AI may include, but is not limited to, unsupervised machine-learning, supervised machine learning, deep learning, reinforcement learning, natural language processing, neural networks, and Generative AI. AI encompasses the idea of machines mimicking human intelligence, whereas non-AI computer algorithms are the specific instructions that enable computers to perform tasks. Algorithms may be a component of AI, used to implement various AI techniques and approaches.

Bribery (Bribe): Any offer, gift, payment, 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 the Mubadala Group.

Business Leader: A senior leader within the business. Names of relevant Business Leaders for Corporate Units, Business Units and Assets are available from the Ethics &

Compliance Office.

Business Partner: Includes any party with which the Mubadala Group conducts business, remits funds to, or receives funds from, including (but not limited to) suppliers, vendors, service providers, consultants, advisors, contractors, distributors, agents, commercial intermediaries, other intermediaries, investors, partners, and mergers and acquisitions targets.

Business Unit: Any subdivision of a Business Platform, which is headed by an Executive Director or any individual designated by the relevant Business Platform CEO to carry out the authorities of such function within their Units.

Charitable Donations: A contribution of any kind to a recognized and legal charity by the Mubadala 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.

Civic Organization: An organization comprised of people who join together to provide a service to their community. A civic organization's sole purpose is to serve a public or mutual benefit other than the pursuit or accumulation of profits; examples include charities, foundations, social welfare and advocacy groups, professional/trade associations, and religious organizations.

Commercial Entity: Any entity that is engaged in business (for profit or not-for-profit) and is not a Government Entity.

Confidential Information: Information acquired in the course of activities for the Mubadala Group that: (a) relates to the Mubadala Group's business or any third-party entity or person; and (b) is non-public or that the Mubadala 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, 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.

Conflict of Interest (or Conflict): Any situation in which a person, or Related Person, has a personal or outside interest that is sufficient to appear to influence the objective exercise of judgement in official duties for the Mubadala Group, regardless of whether it would actually influence that exercise of judgement.

Corporate Unit: Any subdivision of a Corporate Platform, which is headed by an Executive Director or any individual designated by the relevant Corporate Platform Officer to carry out the authorities of such function within their Units.

Corruption: An act done with an intent to give some improper advantage inconsistent with official duty and the rights of others; misuse of a station or office to procure some benefit either personally or for someone else contrary to duty and to the rights of others.

Counter Terrorist Financing (CTF): Tactics, techniques, and strategies designed to limit terrorists' sources of, and access to, funding.

Data Controller: An individual or company who (either alone or jointly with others) determines the purposes for which, and manner in which, any Personal Data are, or are to be, processed.

Data Protection Lead (DPL): A person(s) who manage(s) the functional responsibility for Data Privacy matters for the relevant Asset. This need not be a stand-alone position and may be full-time or part-time, depending upon the risk, nature, and needs of the Asset.

Data Subject: A Person who can be identified, or is identifiable. An identifiable Person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an ID number, location

data, an online identifier or to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Person.

Deal Team: A group of Restricted Persons that have or it is anticipated will receive Material Non-Public Information concerning a specific publicly listed Security(ies) and who, as a result, have been designated as Restricted Persons. Individuals may be part of more than one Deal Team.

Deal Team Lead: An individual responsible for initiating a Restricted Security request for a Deal Team that have or it is anticipated will receive Material Non-Public Information concerning a specific publicly listed Security(ies).

Director: A member of the governing Board of an association, corporation, or other incorporated entity.

Due Diligence: The process undertaken to assess the level of risk posed by a potential Business Partner by gathering, analyzing, managing, and monitoring information about them.

Entertainment: Includes, but is not limited to, travel, sports events, concerts, theater, vacations/holidays, use of corporate assets (e.g., facilities, corporate jet), training events, conferences, and other similar functions and events.

Ethics & Compliance Office: The Mubadala Ethics & Compliance Office or relevant Asset ethics & compliance function.

Facilitating Payment: An unofficial amount paid to a Government Official to expedite a routine function, which they are otherwise obligated to perform (e.g., visa processing, licenses, inspections etc.). A Facilitating Payment is a form of Bribe.

Financial Interest: Ownership of capital stock, bonds, notes, futures, options, or other Securities; partnership interest (general or limited) or other proprietary rights; direct or indirect interest through a trust, nominee, or other relationship; ownership of business property or



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

55

/ 60





real estate (other than a personal or family residence); or any other type of financial relationship with an Outside Concern. 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).

Fraud: Any deliberate act or attempt involving deception, trickery or dishonesty, including misrepresentation that knowingly or recklessly misleads, or attempts to mislead with the intention to cause losses (financial or otherwise) to the Mubadala Group, Mubadala Group Personnel or Business Partners.

Generative AI: AI that can independently create content, such as text, images, music, or even code, by learning patterns from existing data.

Gift: Anything of value, other than Entertainment, including but not limited to, payments (in cash, vouchers, gift cards, bank transfers, rebates or discounts not available to the general public, or other forms), per diems, jewelry, food or beverage (not taken with others as part of an event, e.g., packaged chocolates), flowers, loans, animals, travel (other than Sponsored Travel), employment, and any other type of advantage or thing of value.

Government Entity: (a) The Government of any country or of any political subdivision of any country or collection of countries, e.g., European Union; (b) any branch, agency, committee, commission, or department of any Government; (c) any person or organization authorized by law to perform any executive, legislative, judicial, regulatory, administrative, military, or police function of any Government; (d) any Public International Organization; (e) any political party; or (f) any state-owned or state-controlled enterprise.

Government Official: Includes any of the following:

- Official, employee, or person acting for or on behalf of any Government Entity or Public International Organization

- Political party official or candidate for political office
- 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
- 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

Insider Trading: Buying or selling (whether directly or indirectly) a publicly listed Security while in possession of Material Non-Public Information about the company underlying that Security. The essential characteristic of Insider Trading is that an unfair advantage is obtained from Material Non-Public Information to the detriment of third parties who are unaware of such information and, as a result, the integrity of financial markets and investor confidence is undermined.

Intellectual Property (IP): Refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Investment and Business Planning Committee: The Investment and Business Planning Committee of Mubadala, which is chaired by the Deputy Group CEO.

Investment Committee: The Investment Committee of Mubadala, which is chaired by the Managing Director & Group CEO.

Large Language Models (LLMs): Powerful computer programs trained to understand and generate human language. They can answer questions, write text, summarize information, and hold conversations. These models learn from large amounts of text and are used in many tools and services.

Leadership: The Chief Executive Officer or equivalent of an Asset, a Mubadala Corporate or Business Unit head, or, in each case, a nominated representative.

Material Non-Public Information: Information that: (a) is of a precise nature; (b) relates directly or indirectly to a publicly listed company or any company with a publicly listed Security(ies); (c) has not been disclosed to the public by that company and is not otherwise in the public domain; and (d) would, if it were made public, be likely to have a significant effect on the price of those Securities.

Meal: Food or beverage provided as part of an event or taken with others, distinct from the Gift of, for example, a box of chocolates or a sealed, bottled beverage.

Money Laundering: The process criminals use to legitimize proceeds obtained from illegal activity. Money is “laundered” by passing it through legitimate businesses, and the nature of the financial transaction and the source, origin, and/or owner of the funds is concealed.

Mubadala Group: Only for the Purposes of this Code and its embedded Policies, Mubadala Group refers to: Mubadala Investment Company PJSC (Mubadala); any entity, operation, or investment controlled by Mubadala, which adopts the Mubadala Group Code of Ethics and Policies; and/or any entity, operation, or investment that adopts the Mubadala Group Code of Ethics and Policies.

Mubadala Group Personnel: All individuals who work directly for or represent the Mubadala Group, whether on a temporary or permanent basis, including directors, employees, consultants, secondees, and long-term contractors or any other person or entity whose transactions are directed by, or subject to, their influence or control.

Non-Reportable Securities: Unless otherwise communicated to selected Mubadala Group Personnel, for the purposes of this Policy the following Securities are non-reportable:

- Exchange Traded Funds (ETFs), mutual funds, unit investment trusts (such as UCITS etc.) and similar entities
- Government Securities (treasury Securities, savings bonds and other direct obligations)
- Options on currencies and exchange-traded options on foreign currencies
- Over-the-counter foreign currency options and swaptions
- Cash, “near cash,” and cash equivalents: e.g. bank accounts, certificates of deposit, money market fund shares and commercial paper
- Personal accounts over which the employee has no direct or indirect influence or control (e.g., a Discretionary (or Managed) Account, blind trust etc.)
- US - 529 accounts, 401k retirement accounts or similar in other jurisdictions that can only hold Non-Reportable Securities
- Investments effected pursuant to an automatic investment plan (i.e., regular periodic purchases or sales in accordance with a predetermined schedule)
- Single-facet cryptocurrency.

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.

Outside Concern: Any organization, entity, or group other than Mubadala or its Assets.

Personal Data: Information from which a Data Subject can be identified or is identifiable, whether directly or indirectly. This will include factual information such as telephone numbers, names, addresses, e-mail addresses, photographs, CCTV footage, voice recordings. It will



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page

also include expressions of opinion and indications of intentions about individuals, such as performance appraisals. Information which does not on its own identify a Data Subject will still be 'personal data' if it can be put together with other information which we hold or which could fairly easily get hold of. For example, if Personal Data has been anonymized by Mubadala but we also hold the key to 'de-anonymize' the information or could fairly easily get hold of that key, then the anonymized information will still be Personal Data. Personal Data may also include online identifiers such as IP addressed and cookie identifiers.

Platform IC: The leadership investment committee of any Platform of Mubadala as may be proposed by the BCEO and approved by the IC.

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 associates. These are senior foreign political persons, including:

- a. A current or former:
 - i. Senior official in the executive, legislative, administrative, military, or judicial branch of a foreign government (no matter whether elected)
 - ii. Senior official of a major foreign political party
 - iii. Senior executive of a foreign government-owned commercial enterprise
- b. A corporation, 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
- 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

Privacy Notice: A document or statement to a Data

Subject with regards to how the organization treats (collects, processes, retains, uses etc.) Personal Data.

Processing: Any operation, whether manual or automated, performed on Personal Data, including but not limited to collecting, recording, organizing, storing, adopting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, blocking, erasing, or destroying.

Pseudonymization: The process of replacing Personal Data with a pseudonym, for example, replacing a name with an identification number.

Public International Organization: Multinational institution composed principally of countries or a collection of Governments or other institutions that carries on Government or quasi-governmental activity(ies) or function(s).

Public Occasion: Official public holiday or occasion in the United Arab Emirates, such as Ramadan, Eid al-Fitr, Eid al-Adha, UAE National Day, etc.

Related Person for the Conflicts of Interest Policy: In relation to Mubadala Group Personnel:

- A spouse, child, step-child, grandchild, parent, stepparent, 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, cousin (including adoptive relationships) whether or not sharing the same household.
- Business relationships in which you are a general partner, owner, or take management decisions
- Trusts for which you are a trustee
- Estates for which you are an executor
- Close personal relationships
- Any other person or entity whose transactions are directed by, or subject to, your influence or control
- Related Person for the **Personal Trading Policy:** In relation to Mubadala Group Personnel:

- A spouse, child, stepchild, grandchild, parent, step-parent, grandparent, sibling, mother-or father-in-law, son-or daughter-in-law, or brother or sister-in-law (including adoptive relationships) sharing the same household
- Business relationships in which you are a general partner, owner, or take management decisions
- Trusts for which you are a trustee
- Estates for which you are an executor
- Any other person or entity whose transactions are directed by, or subject to, your influence or control.

Relationship or Account Owner: The individual within the Corporate Unit/Business Unit or Asset who is responsible for forming and managing the relationship with the Business Partner.

Restricted Party(ies): Any party (whether a legal or natural person) that is subject to trade controls, sanctions, embargoes, denied party, or other trade restrictions either individually or by virtue of being resident, domiciled, incorporated, or located in a country that is subject to such restrictions.

Restricted Person(s): Any Mubadala Group Personnel who have been identified as subject to restrictions on their personal Securities trading because they have received or it is anticipated will receive Material Non-Public Information as part of their Mubadala Group duties.

Restricted Security(ies): Securities included on a Restricted Person's Restricted Securities List.

Restricted Securities List: A list of companies whose Securities may not be traded, either directly or indirectly, by Restricted Persons.

Risk Management Policy: A policy outlining the procedures and guidelines for identifying, assessing, and managing risks associated with the use of AI Tools within the organization.

Security(ies): Any publicly-traded or quoted share or

debt instruments, or derivatives or any other financial instruments relating to those shares or debt instruments.

Securities Tipping: Disclosing Material Non-Public Information to any other person, except where the disclosure is made in the normal exercise of an employment, a profession or duties. Securities Tipping includes disclosing Material Non-Public Information to enable another person to trade in a Security on the basis of that information.

Sensitive Personal Data: Personal Data that require enhanced protection due to the delicate nature of the information. This information includes racial or ethnic origin, nationality/passport, political opinions, religious or similar beliefs, trade union membership, physical and/ or mental health information, biometric data, data concerning a natural person's private life, and criminal convictions, allegations, court proceedings, and/or sentences.

Special Category Data: Sensitive Personal Data, the exposure of which could be used for discrimination or could impact rights and freedoms of the Data Subject.

Sponsored Travel & Hospitality: Includes any form of transportation (such as flight tickets and land transportation) and associated hospitality and lodging (such as hotel bookings, meet and greet services, and other related arrangements) that are offered as part of a business-related engagement, such as conferences, site visits, or business meetings.

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.

Terrorist Financing: Financial support of terrorists or those who encourage, plan, or engage in terrorism-related activities.



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

57

/ 60





Home



Code of Ethics



Conflicts of Interest



Anti-Bribery & Corruption



Business Partner Due Diligence



Personal Trading



Data Privacy



E&C Artificial Intelligence



Contact Us



Last viewed page



POLICY DETAILS



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information



Definitions



Policy Details

58

60





POLICY DETAILS

Code of Ethics	
Version	4.1
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

Personal Trading Policy	
Version	3.4
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

Conflicts of Interest Policy	
Version	3.4
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

Anti-Bribery & Corruption Policy	
Version	4.4
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

Data Privacy Policy	
Version	2.4
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

Business Partner Due Diligence Policy	
Version	3.4
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments

E&C Artificial Intelligence Policy	
Version	1.1
Effective Date	August 2025
Next Review	December 2027
Owner	Head of Ethics & Compliance The Policy Owner is responsible for periodically updating and reviewing this Policy to reflect regulatory, best practice and business developments



Leadership Message



Introduction



Culture



Internal Business Conduct



External Relationships



Marketplace Conduct



Information

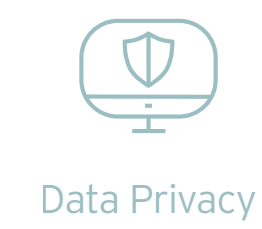


Definitions



Policy Details





CONTACT US

For further information, contact the Ethics & Compliance Office.

Ethics & Compliance Office

+971 2 413 3333

ethics@mubadala.ae

mubadalacompliance.ae



Definitions



Policy Details