# UOB Code of Conduct

Restricted

Version 12

March 2026

# Table of Contents

## CHAPTER 1 – FOREWORD

The UOB values - Honourable, Enterprising, United and Committed – are at the heart of our Code of Conduct which lays down the principles of personal and professional behaviour expected of all UOB employees worldwide.

Honourable, in particular, defines us as a bank. We have always focused on building a sustainable business, by doing what is right for our customers and creating long-term value for our stakeholders. That is why we impress upon all colleagues the importance of upholding the highest professional and ethical standards in their interactions with customers, colleagues and members of the communities in which we operate. Through our consistent and values-led behaviour, we will maintain confidence and trust in UOB.

We will take a strong stance against any behaviour that undermines the strong reputation that we have built over more than nine decades. UOB has a zero-tolerance approach to bribery and corruption, and all other illegal or unethical behaviour. All colleagues across our global network are expected to be in full compliance with all applicable laws and regulations. Where relevant, the same standards apply to those who represent us – from agency staff to vendors.

At the workplace, we promote an inclusive culture where everyone is treated fairly and with care and respect. UOB is committed to ensuring equal opportunity based on merit and to ensuring a safe working environment that is free from discrimination, bullying and harassment.

Each of us has a responsibility to uphold the UOB Code of Conduct and play our part in upholding individual accountability and standards of conduct in UOB. It is mandatory to apply its principles to your everyday actions.

I trust that everyone will do what is right for our customers, colleagues and UOB.

Hendra Gunawan
President Director UOB Indonesia

March 2026

## CHAPTER 2 – INTRODUCTION

We expect that all our Employees and, where applicable, our third-party Business Associates to act in accordance with the highest standards of professional and ethical behaviour, as defined in this **UOB Code of Conduct** (the "**Code**").

The Code is integral to our Risk Culture and outlines the expectations and responsibilities that guide our decision-making and actions. Adhering to it safeguards the trust our customers place in us, protects our franchise and upholds the reputation we have built over time. It is designed to help us understand our responsibilities and obligations, and to provide direction when faced with ethical and professional dilemmas, including conflicts of interest. This includes expectations for responsible business conduct, encompassing business ethics, regulatory compliance, respect for internationally recognised human rights, and the protection of our colleagues, customers and the wider community.

All individuals working for or in connection with us, including but not limited to Board of Commissioners, Board of Directors, managements and non-executives both working on a full-time and part-time basis, temporary employees such as trainees and interns ("**Employees**" for the purpose of this Code only) and where relevant, third-party independent contractors, agents, agency staff, consultants, vendors and suppliers of goods and services ("**Business Associates**" for the purpose of this Code only)[1] are subject to the Code, in addition to all other applicable policies or standards established by UOB and the local laws in the jurisdictions in which we operate must be followed. Where applicable, Employees must ensure that the relevant UOB policies or standards and local laws are made known to their Business Associates for compliance.

As a matter of practicality, the Code cannot possibly cover every policy, procedure and industry guideline. All Employees and Business Associates are expected to apprise themselves of all relevant information, including applicable UOB Policies related to their job functions and to carry out their responsibilities honestly, in good faith and with integrity, due care, competence and diligence. We also regularly review our operations to identify potential risks and issues, including in relation to human rights, and provide confidential and secure mechanisms for Employees to raise their concerns.

This Code supersedes the previous versions issued.

The Code can be viewed on the UOB portal.

**Important Notice:**

*Employees should read the Code in conjunction with the local laws of Indonesia. This also includes the Code of Conduct applicable to the banking industry in Indonesia, such as The Association of Banks in Indonesia, Code of Conduct for Banks and Bank Staff. Where the local laws, regulatory requirements or banking practices of Indonesia impose a higher standard than this Code, then such local laws, banking practices and/or regulatory requirements must be complied with. The Code and other applicable UOB policies and procedures may be updated or amended from time to time, and Employees are required to update themselves of these changes, and to comply with all changes accordingly.*

## CHAPTER 3 – OUR PEOPLE

*Honourable behavior is one of UOB's core values. Employees are expected to lead by positive example and to observe rules and spirit of the Code and applicable Laws. In practice, this means each of us must respect the rights and dignity of one another and help create a safe working environment free from discrimination and harassment, where personal data is handled with care and protected. It is also important that Employees undergo regular training, cooperate fully with authorised external and internal investigations and refrain from hedging of variable pay.*

### 3.1 Discrimination, Harassment

We are committed to respecting your rights and fostering a safe and harmonious working environment where Employees are treated fairly, encouraged to develop their skills and rewarded on the basis of individual and team performance. We are equally committed to ensuring equal opportunity for all based on merit. We take guidance from local fair employment practices and internationally accepted human rights principles and standards, such as the Universal Declaration of Human Rights, United Nations Guiding Principles on Business and Human Rights, and International Labour Organisation Declaration on Fundamental Principles and Rights at Work.

We do not tolerate discrimination or harassment, whether through physical, digital or verbal means, by anyone including you, your supervisors, vendors, contractors or our customers. This applies whether the behaviour occurs on or off the workplace at business-sponsored social events or on any occasion where UOB is represented. Such behaviour is inconsistent with our core value of honourable behaviour and our long-standing tradition of providing a respectful, professional and dignified workplace.

Discrimination is unacceptable, including behaviours which target a person's race, ethnicity, gender, gender identity or expression, colour, creed, religion, national origin, nationality, citizenship, age, disability, marital status, sexual orientation, culture, ancestry, veteran status, socioeconomic status, pregnancy, caregiving responsibilities, language ability, mental health condition or any other legally protected characteristic.

Harassment is equally unacceptable, including the behaviours that undermines the dignity of individuals in the workplace, or is personally offensive, or fails to respect the rights of others, or disregards the impact such behaviour may have, or creates an unfavourable work environment.

Examples of discrimination and/or harassment include:

- Unwanted physical contact or unwelcomed sexual advances
- Display of sexually suggestive images, objects or written materials
- Insults and obscene language
- Sexually explicit or racially offensive jokes/comments
- Excluding or victimising someone
- Conduct that denigrates or ridicules intimidates or physically abuses someone due to their background, culture or ethnicity, sex, race or disability
- Cyber bullying
- Stalking

UOB embraces diversity that spans gender, culture, ethnicity, nationality, experience and skillsets. Creating and maintaining a supportive work environment where every individual can succeed in their career is a critical part of company's strategy to serve the needs of Bank's diverse customer base. In this regard, supervisors must not abuse authority, including compelling their employee to act against UOB values or in ways that contradict the principles laid down in the Code. UOB will continue to recruit, retain, develop and reward the best talent for company, without prejudice.

UOB is subject to Law no. 39 of 1999 concerning Human Rights and any similar laws in.

**Q&A**

Q: I feel uncomfortable and threatened by how a colleague talks to me. What should I do?

A: You are encouraged to discuss any issues, complaints or suggestions concerning your job or workplace to your supervisor or function head in accordance to company's Collective Labor Agreement and not express them in public settings or online platforms.

### 3.2 Conducive and Healthy Environment

The Bank is committed to conducting its business in a way that upholds the safety and well-being of its Employees, customers, Business Associates and the environment. This means that everyone's behaviour contributes to a positive and healthy workplace wherever we operate.
It is essential that Employees and Business Associates to act in accordance with the laws of the jurisdictions:

- Do not engage in criminal or illegal activity. You must abstain from the misuse of drugs while conducting business for the Bank, at the workplace or on your personal time You must not possess, use, distribute, or sell any items that are prohibited under local law, including but not limited to illegal drugs, vaping devices, or any other contraband.

- Employees and Business Associates must always keep their judgment clear and unimpaired from the misuse of drugs or alcohol at all times. If there is a formal activity/event determined by the Company involving alcohol/liquor consumption, this requires the approval of the Country Function Head/ Regional General Manager (RGM) for the Branch office via email and consumption must be carried out within reasonable limits applying the principles of objectivity and professionalism. Charging for alcohol/liquor follows the provisions of the Request, Procurement and Payment Procedures applicable in the Company.
- Comply with all relevant health and safety laws and guidelines and promptly report any condition that may pose a health, safety or environmental hazard to their immediate supervisor and/or Human Resources.

- The Company prohibits betting and/or gambling of any form in the office or within Company's premises, and on any occasion where they are or may be representatives of the Company.

Employees to comply with the UOB Facilities Management & Workplace Safety and Health Policy which can be found on the UOB Policy Portal in the intranet.

### 3.3 Protection of Personal Data

UOB regards the lawful use and handling of personal data to be of utmost importance. “Personal data” includes, but is not limited to:

a. Specific personal data; and
b. General personal data

Specific personal data includes:
a. health data and information;
b. biometric data;
c. genetic data;
d. criminal records;
e. children data;
f. personal financial data; and/or
g. other data in accordance with the provisions of laws and regulations.

General personal data includes:
a. name;
b. gender;
c. citizenship;
d. religion;
e. marital status; and/or
f. personal data combined to identify an individual.

The Bank carries out Personal Data Processing as referred to in Law No. 27 of 2022 concerning Personal Data Protection, which includes (i) obtaining and collecting, (ii) processing and analysing, (iii) storing, (iv) correcting and updating, (v) displaying, announcing, transferring, disseminating, or disclosing, and/or (vi) deleting or destroying, and in accordance with the Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 concerning Personal Data Protection in Electronic Systems and other relevant Laws or Regulations.

UOB manages your personal data in accordance with the UOB Privacy Notice (Employees).

Employees and Business Associates may have access to personal data while performing their duties. If we are in possession of personal data, we must protect the confidentiality of the data and should never use it to benefit ourselves or any third party. This includes handling personal data carefully as to prevent unauthorised access or disclosure, and using secure methods to transfer, store and dispose of it. Employees should regularly

review personal data in their possession and delete those that are no longer needed. Employees and Business Associates should only access or use personal data to perform job-related duties, and not share it internally or with external third parties, unless authorised to do so. Discretion must also be exercised when sharing personal data via the bank's collaboration sites, e.g. email, SharePoint, Teams, to ensure that this is strictly on a need-to-know and need-to-have basis.
For further information regarding the processing of personal data, refer to the Personal Data Protection Policy available on the Company Portal.

### 3.4 Training

UOB provides an array of learning programmes (e.g. instructor-led workshops, self-directed digital online learning, seminars and conferences, on-the-job learning) to help you maintain and enhance the competence, knowledge and skills to effectively carry out your roles and responsibilities with the Bank. You must not misuse the learning and development resources provided by the Bank for personal gain and/ or benefits.

You must complete all required training identified by the Bank such as annual refreshers or mandatory new employee training during induction. The scope may include, but is not limited to:

a. Code of Conduct
b. Fraud Awareness
c. Information Security
d. Operational Risk Management
e. UK Bribery Act 2010
f. Fair Dealing Guidelines
g. Anti-Money Laundering/Countering Financing of Terrorism/Sanctions
h. Sustainability

When attending learning programmes that involve external personnel (e.g. training vendor, course mates), you must exercise due care to prevent unauthorised disclosure of customer's or bank's proprietary data (including non-customer personal information)

### 3.5 External and Internal Investigations

UOB is accountable for upholding the highest standards of ethics and integrity. Employee must cooperate fully with any authorised external or internal investigation, both during and after their employment or engagement with UOB. Refusal to provide evidence, hampering investigation processes, making false, misleading or malicious statements, tipping off others or unauthorised disclosure of an investigation, and tampering with evidence are grounds for disciplinary action, including the termination of employment or other relationships with UOB.

Employee must inform their supervisors, Human Resources and Legal immediately if they are contacted as part of any external investigation by law enforcement agencies, or governmental or regulatory authorities.

For more information on fraud-related investigations, please refer to Anti-Fraud Policy applicable in the Company.

### 3.6 Hedging of Variable Pay

For better clarity between misconduct risk and remuneration and for effective risk alignment in line with regulatory requirements, Employees are prohibited from using hedging strategies or compensation-and-liability-related insurance or other similar financial instruments to protect against, or to compensate for:

- any adjustment, reduction or loss in variable pay or incentives;
- any forfeiture of unvested and/or deferred variable pay or incentives; and
- any clawback of vested or paid compensation (e.g. paid variable pay, incentives or vested deferred variable pay either in cash or equity).

## CHAPTER 4 – OUR CUSTOMERS

*In line with our core values, we stand united with our customers and remain committed to delivering excellent service. Treating all customers fairly and with respect, keeping their information confidential, and maintaining our professionalism, independence and objectivity is central to UOB's way of working. To protect our customers, we conduct appropriate due diligence on products and services before offering them to our customers.*

### 4.1 Treating Customers Fairly

We are committed to building trusted, long-lasting relationships with our customers, grounded in mutual respect, active partnership and long-term commitment. Treating our customers fairly is integral to providing excellent customer service.

Our value of Honourable reinforces our dedication to delivering the five fair-dealing outcomes outlined:

- Outcome 1: Customers have confidence that they deal with financial institutions where fair dealing is central to the corporate culture.
- Outcome 2: Financial institutions offer products and services that are suitable for their target customer segments.
- Outcome 3: Customers are served by competent representatives.
- Outcome 4: Customers receive clear, relevant and timely information that accurately represent the products and services offered and delivered.
- Outcome 5: Financial institutions handle customer complaints in an independent, effective and prompt manner.

### 4.2 Protecting Customers' Information

UOB is committed to protecting customers' information and using it appropriately, in accordance with applicable privacy of customer information, privacy and data security laws and regulations, contractual obligations and our policies and procedures.

Safeguarding customer data and maintaining its confidentiality are essential to preserving the trust and confidence placed in us. Any wrongful use or disclosure of customer data may undermine customers' trust in UOB, result in regulatory penalties, lead to possible legal action and harm the Bank's reputation.

Disclosure of customer information within the organisation must be strictly limited to a need-to-know basis. Discretion must also be exercised when sharing customer information via the bank's collaboration sites, e.g. email, SharePoint, Teams, to ensure that this is strictly on a need-to-know and need-to-have basis. Accessing customer information out of curiosity, for personal reasons, or for the benefit of third parties is strictly prohibited.

Customer information should not be shared with another customer, any employee, officer or shareholder of a customer, or any third party, beyond approved job scope or without specific authorisation. Discretion must be exercised when discussing a customer or other confidential information, to ensure that there is no inadvertent disclosure to others nearby who may not be authorised to know that information, both when in the office and especially in public settings.

We are subject to national and local laws, regulations and risks that vary from one country to another. The classification of information as “customer” or “business” data may differ depending on the legal requirements in each countries. “Customer” includes past, present and prospective customers. Some examples of customer information and business data are:

***Customer information***

- name
- date of birth or age
- biological mother’s name
- identification or passport number
- personal financial information including account and transaction details
- business plans
- health
- family matters
- contact details including telephone numbers, email address and home address
- other data submitted or given access by the customer
- gender
- citizenship
- religion
- marital status
- biometric data
- personal data combined to identify an individual

***Customer business data***

- business plans
- transactions including credit facilities
- financial information of corporate clients, Business Associates and other third parties

Communications with customers should always be sent using enterprise accounts through approved channels to the designated contact information (e.g. email, phone number, address) provided by customers as maintained in the Bank’s system.

Contact information should be carefully checked to ensure that documents are sent only to the intended recipients and appropriately protected to avoid unauthorised disclosure of information. Customer information should not be sent to your personal email address, even for work convenience. For more information, please refer to Information Technology Security Management and Cyber Resilience Policy.
Non-compliance–including wrongful disclosure or use of customer information after employment termination with the Bank–may be a criminal offence in certain jurisdictions, punishable by fine and/or imprisonment. Offenders may also be subject to civil liability.

Ignorance of confidentiality or data privacy laws is not an acceptable reason for non-compliance. You are to be familiar with the laws applicable to your work in the country.

As legal requirements vary across jurisdictions, you should consult your local Data Privacy Risk & Compliance and Data Protection officer before disclosing any customer information to a third party. If there are different laws regarding Customer Data Privacy based on the entity, please refer to the guidelines located on the Intranet.

**Q&A**

Q: A Financial Advisor received a phone request to forward financial information to the customer's spouse's email address. However, the Bank procedure states clearly that all email communications should be sent to customer's email address maintained in the Bank's system. Is it fine to make an exception this time since this request comes directly from the customer?

A: No, the Financial Advisor should not use an email address given over the phone call. If the customer was unable to access his pre-registered email, he should follow the process to initiate a change of pre-registered email.

### 4.3 Maintaining Professionalism, Independence and Objectivity

We must always exercise reasonable care and judgment to prevent, avoid and proactively address circumstances that threaten or appear to threaten our professionalism, independence and objectivity. We should never place ourselves in a position where our ability to conduct business in an ethical manner may be or appears to be compromised, or where our action(s) may violate the law or UOB policies and standards.

Some examples of unacceptable conduct and prohibited sales practices are:

- using your own or your family member's personal address and contact number as contact details for any customers' or prospective customers' accounts.
- trading in any shares/stocks/investments on behalf of customers even if customers give the mandate to act on their behalf.
- allowing your bank account to be used by customers. Employees should not allow their bank accounts to be used by customers or to receive customers' fund for whatever reason.

Any of the above actions may unknowingly endorse criminals in their conduct of criminal activities that include but not limited to fraud and money laundering.

If you are found to have engaged or attempted to engage in any unacceptable conduct or prohibited sales practices, you may be subject to disciplinary action, which could include termination of your employment with UOB.

**Q&A**

Q: Lunar New Year is just round the corner and my customers request me to help them change new notes. They will transfer the money to my personal bank account for this purpose. Is this allowed?

A: No, you should not allow your bank account to be used by customers or to receive customers' monies for whatever reason.

**Q&A**

Q: A customer of mine asks me to help her make down payment to her car dealer for a new car that she is purchasing as she is currently out of town. She suggests transferring the funds to my personal bank account to facilitate the payment. Should I help her as suggested?

A: No, you should not allow your bank account to receive customers' monies for whatever reason. Instead, you should suggest to your customer to arrange for a family member to make the down payment to her car dealer on her behalf.

## 4.4 Ensuring Proper Governance and Due Diligence on Products/Services Offered

UOB is committed to protecting our customers by conducting thorough due diligence on products and services prior to their launch to address all associated risks and to ensure that they are suitable for the targeted customers. Employees must not advise, recommend or promote any products or services which are not approved by the Bank.

All products developed by UOB, including third-party products marketed using UOB's name, are to undergo the product approval process in accordance with the Bank's Product/Service Programme Policy before these products being offered to customers.

Policies and guidelines within business units relating to products and services offered must be adhered to.

For more information, refer to Product/Service Programme Policy available on the UOB portal.

## CHAPTER 5 – COMPANY'S ASSETS

*UOB protects its intellectual property and respects the intellectual property rights of others. We must use company assets only for official purposes and in the interests of the Company. We must also ensure that we keep proper records as well as handle and dispose records properly.*

### 5.1 Company Information

Employees and, where appropriate, Business Associates must always keep business information confidential. This includes outside the workplace and working hours, and even after the departure of the Employee or the end of the engagement with UOB.

Such information includes, but is not limited to:

- customer information
- internal policies and procedures
- human resources and employee salary and benefits information
- business strategies and plans, including information relating to pricing and products, until such time when they are made public
- other proprietary information acquired during the course of the Employee's or Business Associate's work

Communications of such information should always be sent using enterprise accounts through approved channels to the designated contact information (e.g. email, phone number, address) provided by customers as maintained in the Bank's system. Employee must not send such information to personal email or instant messaging account for any unauthorised purposes. Discretion must also be exercised when sharing classified company and business information via the bank's collaboration sites, e.g. email, SharePoint, Teams, to ensure that this is strictly on a need-to-know-basis.

Business information should not be uploaded to unauthorised internet platforms, including public generative artificial intelligence (AI) tools or language translation websites, whether accessed through personal or Bank-issued devices. Doing so may lead to a breach of privacy of customer information set out in the Personal Data Protection Act.

### 5.2 Intellectual Property

The owners of intellectual property have rights granted to them under the law. Intellectual property includes, but is not limited to, patents, industrial designs, user interface, trademarks and copyrights.

Any intellectual property developed or acquired by UOB is company property, and we must make every effort to secure and protect our interests in this regard and should not without proper authorisation, disclose, use or allow a third party to use it, during or after their employment with the Bank.

We must also respect the intellectual property rights of others, such as our customers, and not use intellectual property obtained in the course of our employment with another company without first having obtained that company's written consent.

UOB respects the limitations placed on third-party software by the software developer and/or distributor. Employees must always use software in the manner specified in the licensing agreement.

**Q&A**

Q: I was previously employed by a competitor of UOB and want to use intellectual property obtained in the course of that employment to bring in new clients for UOB. Is this allowed?

A: No. UOB recognises and respects the intellectual property rights of all third parties – whether they are a direct competitor or not is immaterial. Written permission must be granted by the owners of the intellectual property before you can use their intellectual property. Similarly, we should always make every effort to secure our interests in intellectual property. At the same time, we should never disclose or use the intellectual property during or after our time of employment with UOB, without proper authorisation.

### 5.3 Use of Bank's Information Technology Assets

UOB's computers, software (whether installed on UOB's computers or electronic devices), networking resources, electronic communications systems including e-mail, instant messaging, telephone, voice systems, communication and virtual conference collaboration platforms, and other computer-processed information (collectively, "Information Technology Assets") are the property of UOB and should be used strictly for delivering UOB's services and products.

Security is everyone's responsibility at UOB. Good security practice is the best way we can protect all of us, our customers' and our information assets, and the valuable information we create and use during our business.

It is important that Employees and Business Associates always follow UOB policies, standards and procedures to safeguard information assets against loss, theft or any type of compromise. Each of us is accountable for the information assets entrusted to our care and we should ensure these are used responsibly, appropriately and ethically.

The secure use of Information Technology Assets is governed by UOB Information Technology Security Management and Cyber Resiliency Policy. To protect these assets, we must be familiar with and always comply with the requirements in the policy regarding the acceptable use of user credentials, personal computing and mobile devices, internet and email usage. In addition, we must also be familiar with any other relevant Information Technology security policies and standards applicable in the course of our work.

UOB reserves the right to monitor, record and audit an Employee's or a Business Associate's use of Information Technology Assets if there are reasonable grounds to suspect illegal or other inappropriate conduct.

For more information, refer to Technology and Operations' Information Technology Security Management and Cyber Resiliency Policy available on the UOB Portal in the intranet.

### 5.4 Accurate Records, Records Retention, Proper Handling and Disposal of Records

UOB business records must always be prepared accurately and reliably. We must ensure that business records are complete, correct, present a fair view of our business and are retained for the period required by law and/or regulation. Information reported and recorded by Employees and Business Associates for UOB's purposes or for use by third parties must be reported or recorded honestly and accurately, with appropriate supporting documents where applicable. It is important that we never tamper with or falsify information on any record or document. Bank records should not be moved, modified or disposed of, except with proper authorisation. We must ensure that our records are of a high standard so that fair and accurate books are available for audit and inspection.

All Employees and Business Associates are responsible for protecting the confidentiality of bank-related and customer records acquired and created in the course of our work in accordance with the Information Classification and Protection Standards. Customer information should not be left unattended to prevent inadvertent exposure of customer information. The same level of care should also be taken in disposing such records when they are no longer required to be retained. It is important to note that customer's confidential information picked up by any unauthorised persons through improper handling or disposal of records could constitute a breach of privacy of customer information as well as Personal Data Protection Act. Misconduct relating to breach of confidentiality will result in disciplinary action.

Employees and Business Associates play an important role in reporting data breach. When Employees or Business Associates become aware of a potential or actual data breach, they are required to promptly manage the data breach and timely report the incident in accordance with Personal Data Protection Policy available on the UOB Portal in the intranet as well as the Data Breach Incident Management Procedures and Incident Reporting Guidelines.

Employees and Business Associates must always comply with all applicable laws and any relevant records management policies or procedures as implemented by UOB. All "*off the record*" accounts or transactions in relation to improper payments are prohibited. Records and data must also be preserved and destroyed in accordance with relevant laws, regulations and UOB records management policies or procedures.

For more information, refer to Document/Archive Management Policy and Procedures and Document Retention Period Guidelines available on Portal.

When Employees are aware that any documents, records or data are, or may be, required for the purposes of legal action or investigation must promptly notify and consult with Legal and any department in the Bank charged with assisting such investigations, and provide

the documents, records or data as necessary. Failing to maintain such documents, records or data, or destroying, concealing or altering them, may result in criminal and civil proceedings against UOB and the Employee(s) concerned.

## CHAPTER 6 – OUR FRANCHISE

*All Employees must seek to protect UOB's franchise value; know and comply with the laws and regulations of the countries in which they operate; avoid conflicts of interest; and reject bribery and corruption. We must never engage in insider trading.*

### 6.1 Insider Trading

UOB has an integral role in ensuring the integrity of the financial system. When in possession of inside information, we must not trade in the related securities (for instance, shares or options), securities-based derivatives contracts or units in a collective investment scheme or disclose such information to family, friends or any other person.

Inside information refers to non-public information that is not generally available and, if it were generally available, a reasonable person would expect the information to have a material effect (whether positive or negative) on the price of UOB securities or the securities, securities-based derivatives contracts and units of a collective investment scheme of other companies, or that the information could influence persons in deciding whether or not to subscribe for, to buy or to sell those securities.

Some examples of inside information are:

- financial results
- major acquisitions, divestments and/or mergers
- major joint ventures
- significant capital projects
- significant contracts
- takeover bids

We must ensure that we handle such information with the appropriate care. Insider trading and tipping off or passing on non-public price-sensitive information is unethical and an abuse of confidential information. You should be aware that in most jurisdictions, insider trading is a criminal offence surmountable to a fine and/or imprisonment.

For more information, please refer to Personal Trading Policies and Procedures for Securities which can be found on the UOB intranet.

### 6.2 Conflicts of Interest

A decision to transact business with any party must be based solely on business considerations, free from bias and in the best interests of UOB. We must always ensure our personal activities and interests and financial condition do not conflict with our responsibilities to the Bank. We must not knowingly permit ourselves to be placed in a position where our interest is or could be perceived as adverse or potentially adverse to the Bank.

If you think that you could be in a conflict of interest situation, you should immediately disclose all relevant details to your supervisor or senior management, as appropriate.

If you are aware of any conflict of interest that involves your colleagues, supervisors or senior management that is not disclosed or resolved, you may wish to report it through our Whistleblowing Hotline.

Employees should advance UOB's legitimate interest when the opportunity to do so arises. At the same time, Employees must never take for themselves (or direct to a third party) a business opportunity that they have discovered using corporate property, information or position, unless UOB has already been offered and has declined the opportunity. Employees should not use or disclose any information obtained in the course of their employment, for the benefit of themselves or a third party.

As it is impractical to describe every potential conflict of interest in the Code, Employees must exercise sound judgment and adhere to the highest ethical standards in conducting both professional and personal affairs. We must always maintain a sound personal financial condition and avoid situations that may prevent us from carrying out our responsibilities to the best of our ability. Employees who have dealings with licensed and/or unlicensed moneylenders must declare their debts and financial condition to Human Resources immediately. Employees should also not conduct transactions with customers outside of the Bank's business or facilitate the entering into of transactions between customers and third parties.

Business units may have specific policies or guidelines regarding potential conflicts of interest, and it is the Employees' responsibility to know and comply with them.

UOB has in place a system of policies, procedures and internal arrangements (including physical separation and Chinese Walls) to restrict the flow of information between and within different business units. These arrangements are designed to prevent improper use or the perception of improper use of client information or other types of proprietary information.

You are to adhere to our policies and guide to ensure that transactions with Related Parties are conducted free of conflicts of interest and based on terms and conditions that are not more favourable than similar transactions with non-related parties under similar circumstances.

### 6.3 Gifts and Entertainment

There is a risk that the inappropriate provision of gifts and entertainment can be used to influence improperly a business outcome or could result in the conferring of an unfair business advantage or create an inappropriate expectation or wrong impression that could constitute a bribe. Employees should exercise good judgement in line with our guidance when offering or accepting gifts and entertainment to/from parties whom they have official dealings with to avoid a situation of actual or perceived position of compromise or conflict of interest. When in doubt, Employees should seek approval from the segment or function head (case-by-case basis) or an authorised officer appointed by the segment or function head (case-by-case basis).

"Gifts" include, but not limited to, money, goods, services or loans given ostensibly as a mark of friendship or appreciation. The term could also refer to favours, advantages and

preferential treatment, as well as any form of entertainment provided to the recipient where the giver is absent.

"Entertainment" may include, but not limited to, meals, expenses-paid overseas trips, or tickets to movies, musicals, social or sporting events where the giver is present at the function with the recipient with the ostensible purpose of building a relationship. When the giver is absent, entertainment should be treated or declared as a "gift".

The general test on whether the gift or entertainment is permissible is whether it is reasonable, proportionate and justifiable in the circumstances. It should not be inappropriate, excessive in value and provided too often as it may leave the recipient in a position of obligation and to induce improper conduct, which could put Employees or the Bank at risk of bribery and corruption.

The guidelines below outline the treatment and declaration of gifts and entertainment. You are to comply with local anti-corruption laws wherever they set a higher standard than these guidelines.

**(A) Gifts**

(i) Circumstances in which you cannot accept a gift include:

- Solicitation of any gift from anyone in connection with work.
- Acceptance of cash gift in connection with work.
- Acceptance of that may give others the impression that our business judgment has been compromised, or that we are under an obligation that conflicts with our duty.
- Canvassing with any external party (for instance, vendors, customers or Business Associates) or any UOB business unit, department, segment, function or entity for contributions, or to sponsor any company, social or staff function with donations in kind or cash.

(ii) You are discouraged from accepting or offering gifts and entertainment from/to parties whom you have official dealings. Exceptional cases may apply as listed below, and a declaration must be made.

- Non-cash gifts (including sponsorships of non-cash gifts for company, social or staff function) that are voluntarily offered by the giver if the value is in line with accepted business practices and cannot be construed as improperly influencing their good business judgment;
- Gifts that are beyond accepted business practices but are justified and approved by the segment or function head (case-by-case basis); or
- Where it is impractical or inappropriate to refuse a gift (including sponsorship of non-cash gifts for company, social or staff function), or where refusal would cause offence or embarrassment or adversely affect the relationship of UOB with the person offering the gift with conditions that the acceptance of gift must not:
- compromise our business judgment;
- put us under an obligation that conflicts with our duty; or
- give such perception.

(iii) You are to adhere to the following guidelines for offering or sponsoring gifts, and the associated declaration:

- All gifts to be offered must be approved by the segment or function head (case-by-case basis) or by an authorised officer appointed by the segment or function head (case-by-case basis).
- Gifts offered must be in good taste and of a reasonable and proportionate value, as determined by accepted business practices.
- Gifts should be given and received openly and must comply with the applicable local laws.
- The intention behind the offering of gifts must be considered carefully. Gifts must not be given with the aim of improperly obtaining or retaining business or a business advantage.
- Within 5 working days, Employee must complete the Declaration of Gifts form (Appendix 1 of the Code) and submit it to the Designated Officer in the Employee's division who handles such matters. If in doubt, the Employee should consult their supervisor or Designated Officer immediately.
- The Designated Officer must verify the contents of the Declaration of Gifts form, record the gift declared in the division's Gift Register (Appendix 3 of the Code) and submit the form to the segment or function head (case-by-case basis) for endorsement.
- The Designated Officer is responsible for maintaining proper records of the division's Gift Register.

(iv) You are to adhere to the following guidelines and procedures for receipt of gifts and the associated declaration:

For any non-cash gift (for example, a souvenir, memento, hamper, discount, rebate, air ticket or gift, dining or shopping voucher) worth S$150 or less, can be reported to his/her supervisor either verbally or in writing and the Employee may retain the gift provided that it would not compromise business judgment. If an Employee is in doubt of the value, he/she should escalate to his/her supervisor or Designated Officer.

For any non-cash gift worth more than S$150, the Employee must follow the declaration procedure below:

- Within 5 working days after gift receipt is obtained, the Employee must complete the Declaration of Gifts form (Appendix 1 of the Code) and submit it to the Designated Officer in the Employee's division who handles such matters. If in doubt, the recipient should consult their supervisor or Designated Officer immediately.
- The Designated Officer must verify the contents of the Declaration of Gifts form, record the gift declared in the division's Gift Register (Appendix 3 of the Code) and submit the form to the segment or function head (case-by-case basis) for endorsement. The segment or function head (case-by-case basis) will decide whether to allow the Employee to retain the gift or to distribute it.

If an Employee receives a gift of cash (such as "red packets") from customers or Business Associates during festive occasions like Lunar New Year, weddings,

infant full-month celebrations, house-warming celebrations or birthdays ("special occasions"), the Employee must complete the Declaration of Gifts form (Appendix 1 of the Code) and submit it to the Designated Officer in the Employee's division who handles such matters. If in doubt, the recipient should consult their supervisor or Designated Officer immediately. The Designated Officer must verify the contents of the Declaration of Gifts form, record the cash gift declared in the division's Gift Register (Appendix 3 of the Code) and submit the form to the segment or function head (case-by-case basis) for endorsement. The Employee may retain the cash gift if it would not compromise business judgement.

For cash gift that is in excess of S$150 given on such occasions, the Employee must seek exceptional approval from the segment or function head case-by-case basis ) or an authorised officer appointed by the segment or function head (case-by-case basis). The segment or function head or an authorised officer appointed by the segment or function head (case-by-case basis) will decide whether to allow the Employee to retain the cash gift. The Employee must follow the declaration procedure above.

The Designated Officer is responsible for maintaining proper records of the division's Gift Register.

**(B) Entertainment**

(i) Circumstances in which you cannot accept an entertainment include:

- Soliciting entertainment from anyone in connection with work.
- Acceptance of entertainment under circumstances where it may appear to others that business judgment has been compromised, or that would place the Employee under an obligation that conflicted with their duty.
- Canvassing external parties (for example, vendors, customers or Business Associates) or any UOB business unit, department, segment, function or entity to provide or sponsor entertainment for any company, social or staff function.

(ii) You are discouraged from accepting or offering gifts and entertainment from/to parties whom they have official dealings with. Exceptional cases may apply as listed below, and a declaration must be made.

- Entertainment (including sponsorships of entertainment for company, social or staff function) that are voluntarily offered by the giver if the value is in line with accepted business practices and cannot be construed as improperly influencing their good business judgment;
- Entertainment that are beyond accepted business practices but are justified and approved by the segment or function head (case-by-case basis); or
- Where it is impractical or inappropriate to refuse entertainment or where refusal would cause offence or embarrassment or adversely affect the relationship of UOB with the person offering the entertainment

with conditions that the acceptance of entertainment must not:

- compromise our business judgment;

- put us under an obligation that conflicts with our duty; or
- give such perception.

(iii) You are to adhere to the following guidelines and procedures for the offering, sponsoring of entertainment and the associated declaration:

- All offers of entertainment must be approved by the segment or function head (case-by-case basis) or by an authorised officer appointed by the segment or function head (case-by-case basis).
- Entertainment offered must be in good taste and of a reasonable and proportionate value, as determined by accepted business practices.
- Entertainment should be provided openly and must comply with applicable local laws.
- The intention behind the offer of entertainment must be considered carefully. Entertainment must not be given with the aim of improperly obtaining or retaining business or a business advantage.
- Within 5 working days, the Employee must complete the Declaration of Entertainment form (Appendix 2 of the Code) and submit it to the Designated Officer in the Employee's division who handles such matters. If in doubt, the Employee should consult their supervisor or Designated Officer immediately.
- The Designated Officer must verify the contents of the Declaration of Entertainment form, record the entertainment declared in the division's Entertainment Register (Appendix 4 of the Code) and submit the form to the segment or function head (case-by-case basis) for endorsement.
- The Designated Officer is responsible for maintaining proper records of the division's Entertainment Register.

(iv) You are to adhere to the following guidelines and procedures for acceptance of entertainment and the associated declaration:

For entertainment (for example, occasional business meal, or ticket to a movie, musical, social or sporting event) valued at S$150 or less, no disclosure is required provided that it would not compromise business judgment. When the giver is absent, entertainment should be treated or declared as a "gift". If an Employee is in doubt of the value, he/she should escalate to his/her supervisor or Designated Officer.

For entertainment valued at more than S$150, the Employee must follow the declaration procedure below:

- Within 5 working days of accepting the entertainment, the Employee must complete the Declaration of Entertainment form (Appendix 2 of the Code) and submit it to the Designated Officer in the Employee's division who handles such matters. If in doubt, the recipient should consult their supervisor or Designated Officer immediately.
- The Designated Officer must verify the contents of the Declaration of Entertainment form, record the entertainment declared in the division's Entertainment Register (Appendix 4 of the Code) and submit the form to the segment or function head (case-by-case basis) for endorsement. The

segment or function head (case-by-case basis) will decide whether to allow the Employee to retain or distribute it (for example, ticket to a movie, musical, social or sporting event).

However, if an Employee feels that the level and value of the entertainment to be provided is likely to be beyond accepted business practices, they should seek guidance from their segment or function head (case-by-case basis) as to whether it is appropriate to accept such entertainment. Examples of entertainment that is beyond accepted business practices and which require the approval of segment or function head (case-by-case basis) or, where appropriate, approval at a higher level, are:

- all-expenses-paid overseas trips where the giver is present
- air ticket(s) or entry to major social, sporting or other overseas event where the giver is present

If the segment or function head (case-by-case basis) approves the acceptance of the entertainment, it must be declared within 5 working days using the Declaration of Entertainment form (Appendix 2 of the Code) and the Designated Officer must record the entertainment in the Entertainment Register (Appendix 4 of the Code). The Designated Officer is responsible for maintaining proper records of the division's Entertainment Register.

## 6.4 Anti-Bribery Laws

Bribery occurs when an individual (directly or indirectly) promises, offers, gives, or seeks, accepts or receives a payment or favour (monetary or otherwise) to improperly influence a business outcome or to confer an unfair business advantage. Bribery and corruption risks may arise during activities, e.g. interaction with public officials and state-owned or state-controlled entities, provision/acceptance of gifts and entertainment, engagement of third parties, hiring, donations and sponsorships.

Anti-bribery laws prohibit companies, and their Employees and agents from using bribery to obtain or retain business or obtain an unfair business advantage. UOB has zero tolerance to bribery and corruption in all forms. Any Employee or Business Associate found guilty of bribery or corruption shall be subject to severe disciplinary action, including termination of employment or termination of contract, as appropriate, and may also be reported to the relevant law enforcement agency for a formal investigation which could potentially be subject to prosecution under applicable anti-corruption laws.

UOB is subject to Bribery Crime Law and Corruption Crime Law in Indonesia as well as other related regulations, including the U.S. Foreign Corrupt Practices Act 1977 and the UK Bribery Act 2010. Both corporates and individuals can potentially be prosecuted for giving or receiving bribes. In most jurisdictions, bribery is punishable with large fines and imprisonment. It is thus important that Employees and Business Associates comply with the applicable local anti-bribery laws, the U.S. Foreign Corrupt Practices Act 1977, the UK Bribery Act 2010 and the Australian Criminal Code ("the Extra-Territorial Laws"), both in letter and in spirit. All UOB Employees should understand that commission of the offences can occur even if they are not physically present in the U.S., UK or Australia.

Where UOB engages a third party to perform services or to act for or on behalf of the Bank, we should look out for “red flags” (Appendix 6 of the Code) which are facts, events, or circumstances, or other information that may indicate a potential concern for illegal or unethical business conduct, particularly with regard to corrupt practices and non-compliance with anti-bribery laws, and ensure that there are procedures in place designed to prevent the third party who act for or on behalf of the Bank from paying bribes which the Bank could be liable for.

Counterparties that are entering into contractual arrangements with UOB must undertake not to engage in or facilitate any business activity that would lead UOB to breach social, regulatory and legal obligations to combat financial crimes including but not limited to bribery.

## 6.5 Facilitation Payments

Certain countries allow what is known as “facilitation payments”–unofficial payments to public officials to secure or expedite a routine service or necessary action to which the payer is legally entitled. Such payments are considered bribes and prohibited by the laws of many countries, including Anti-Bribery Law in Indonesia and UK Bribery Act 2010.

UOB prohibits facilitation payments. If you are in doubt about the legitimacy of a payment that you have been requested to make, including facilitation payments, or have concerns that such a payment may be needed, seek the advice of your segment or function head, who will keep and maintain a central record of any demands for payments.

Employees and, where relevant, Business Associates should make whatever payment necessary to protect their personal safety, and then, as soon as reasonable, report the nature of the incident and related payment to their segment or function head. Each segment or function head will maintain a register of such payments and notify Legal.

## 6.6 External Communication

UOB is committed, in principle and in practice, to openness and transparency in communicating with external audiences and seeks a constructive relationship with key stakeholders (customers, investors, analysts, regulators, government, media, community and non-governmental organisations).

### *(A) Communication with Regulators*

All communication with the regulators must be made in accordance with Compliance’s Guidelines on Communications. Requests from regulators for information should be answered with complete, factual and accurate information.

For more information, refer to the Guidelines on Communications with the regulators on the UOB intranet.

### *(B) Communication with the Media*

All communication with the media must be made in accordance with the Policy on Media Communications. “Media” refers to the medium of mass communications and includes, but is not limited to:

- Print: Newspapers, magazines, journals and newsletters
- Broadcast: Television, podcast and radio
- Online: E-mail, news websites, social media channels, and blogs

Note: media refers to unpaid or earned media. It does not include paid coverage or advertisements.

“Media communications” refers to all forms of engagement regarding and on behalf of UOB and includes, but not limited to:

- News releases and fact sheets
- Speeches and PowerPoint presentations
- Commentaries
- Media interviews, including for publication on digital platforms
- Media briefings
- Media engagement activities
- Media queries and responses, frequently asked questions (FAQs)
- Media infographics
- Media photographs and video news releases

In-country Strategic Communications and Brand (SCB) is the primary contact for all media engagement and media communication activities. They are the only functions in the Bank permitted to distribute materials to the media.

All media queries received by Employees should be directed to SCB. Do not provide comment to the media in any way (including saying ‘no comment’).

If in doubt, please contact SCB Head or Communications Head UOB Indonesia, or you can also send an e-mail to DL-SCB.

Only President Director, Board of Directors, Segment and Function Heads, as well as their approved alternates, are authorised to speak with the media on their approved areas of expertise or topics and within the approved geographical coverage. All media content must be cleared with SCB and President Director prior to distribution/release to the media and public.

All identified spokespeople are required to complete a media training course arranged by SCB.

For more information, please refer to SCB's Media Communications Policy.

### *(C) UOB Protocol on the Use of Social Media and Online Behaviour (“Protocol”)*

**Purpose**

**This section should be read in conjunction with the UOB Indonesia Social Media Usage Policy, which details the operating standards on the management and use of social media.**

The Internet has become one of the most important communication tools used by individuals and companies today. The influence of the Web and social media on our daily lives brings new opportunities and risks that need to be understood for the tools to be used responsibly and for results to be achieved optimally.

UOB has developed this Protocol to guide Employees on the appropriate and responsible use of social media, both personally and professionally. Employees are responsible for their actions on social media. UOB will not be held liable for the actions carried out by Employees on social media.

Think before you post online. Once your post is sent into the digital world, it is there forever. You need to be mindful that whatever you post online can impact UOB's reputation, its business and your own personal reputation.

When in doubt, please contact the Social Media Unit (SMU) in Strategic Communications and Brand (SCB).

## Application

This Protocol applies to all Employees of UOB and its subsidiaries.

## Scope

This Protocol applies to online behavior in the use of all forms of internal and external social media including, but not limited to:

- Internal platforms, such as MyUOB, Viva Engage and Microsoft Teams;
- Social networking sites, such as Facebook, and LinkedIn;
- Messaging apps, such as Facebook Messenger, LINE, WeChat, WhatsApp, Telegram;
- Video and photo sharing websites, such as Instagram, Snapchat, TikTok, Flickr and YouTube;
- Micro-blogging sites, such as Twitter/X;
- Blogs and websites, including personal and corporate blogs and websites;
- Forums and discussion boards, such as Kaskus and Yahoo! Groups, or those related to online news media; and
- Online encyclopaedia, such as Wikipedia.

## Key Principles

1. As Employees of UOB, we have a shared responsibility to promote and to protect the Bank's reputation in the physical and virtual worlds by upholding UOB's values and behaving in a legal, moral and ethical way.

2. Employees should also be aware that all forms of digital communication (including but not limited to those on websites, mobile apps and social media platforms, etc.) can be traced back to its author and what one does on social media can easily be made public, even if the actions had been carried out on an internal platform or a private account. Once an action has been taken in the virtual world, the digital trace can remain available even after deletion as the content may already have been captured as a screenshot or stored on a cache site.

   While privacy settings on social media networking sites can limit the visibility of the content to an intended set of audience, this will not prevent the intended audience to share such content with non-intended parties. As such, Employees should be aware that actions taken online can no longer be "gated" or kept contained.

3. Employees are encouraged to 'like' and to 'share' content posted on official UOB social media accounts. Employees may also add positive commentary (except on content related to products and services) that is not a promotion. Such content may include, but are not limited to, corporate announcements and updates, product and service updates, employee highlights and feature stories, CSR activities, etc., that are posted on official UOB social media accounts on platforms including, but not limited to Facebook, LinkedIn, YouTube, LINE, WeChat, etc.

4. Employees who notice negative mentions of UOB or any activities that could potentially be a risk to UOB on any websites or social media accounts should also report these to the SMU for the assessment on the action required. Do not circulate such content further.

5. Employees who would like to indicate their employment with UOB should use their actual corporate title on social media/professional networking sites/recruitment sites (e.g. LinkedIn). Do not misrepresent yourself. In addition, companies need to be careful when listing personal information such as mobile phone numbers and email addresses on social media/professional networking sites to reduce the risk of becoming a phishing target.

6. Where applicable, Employees should clearly express that all views are their own and not that of UOB. Employees' personal points of view and actions may be perceived as representative of UOB by virtue of their association with UOB; therefore, Employees need to be mindful that their actions, choice of words and visuals can have a direct impact on UOB.

7. Employees should respect copyright laws and not upload or post any content – including text, videos, photos and images – belonging to someone else, unless they have the appropriate rights to do so.

8. Employees should always provide the reference of, or credit the source when sharing content from an external party.

**Protocol**

It is important for Employees to use social media in a responsible manner when operating their personal social media accounts, and to be guided by the following best practices in their online behaviour.

***1. All work-related policies apply online, including confidentiality and privacy policies***

a. All confidentiality and privacy policies related to the Banking Act, the UOB Code of Conduct, and Indonesia Code of Conduct for Banks and Bank Staff apply to Employees' online behaviour.

b. Policies on Employees' access and use of social media.

c. Employees may blog or discuss topics related to their work at UOB on social media, or post content taken at private work-related events, including but not limited to, Customer/Client events, Townhalls, Annual Dinner and Dance, Team activities for work etc, if they adhere to guidelines set by SMU.

d. However, in relation to paragraph 1(c), Employees are not allowed to post, to share or to distribute, in any form, any content that pertains to materially sensitive company information, any information classified as SECRET or CONFIDENTIAL, non-public, proprietary information, or regarding UOB or its clients, online or on social chat groups and other forms of social media. This includes, but is not limited to, UOB financial information, Customers or Employees' information, future business performance, business plans, directives, functional instructions, internal and non-public events, information on the departure of senior executives, client confidences, messages from senior management and information available to Employees on the UOB intranet.

e. Employees are allowed to post content taken at UOB's public events but should ensure their actions are done to promote and to protect the Bank's reputation, and that they have the necessary permissions to use the source(s). For example, if you are using copyrighted material, seek written approval from the content owner through an email or a signed memo. An exception may be granted if the owner expressly permits all attendees to post the content during the event.

f. Employees are advised not to take photos or videos at working spaces in the workplace and post them on external social media. This includes internal meeting rooms, offices, bank vaults, server rooms etc. They may only do so if it is for use on official social media accounts. Areas in the workplace that may be shared on social media include common spaces like pantries, breakout area and engagement area. Employees should exercise caution when posting images on social media and ensure that no information related to paragraph 1(d) is shared.

**Examples:**

- **Do** post content from events open to the public such as the UOB Heartbeat, UOB Economic Outlook, Public Seminar/Forum, Press Conference, Public Talk Show, CSR events on your personal social media accounts, but ensure that whatever you post is done in a responsible way that will not put anyone, including the Bank, in a bad light. To ensure that the use of words, photos including photo poses follow ethical standards in speaking, are polite and professional.

- **Do Not** post a candid photo or video of President Director taken at a company event or extract a quote sent by President Director through internal communication channels to Employees and post it on Twitter/X.

2. ***Do not sell or market UOB products, or provide financial advice on social media***

   a. Employees are not allowed to create or to use UOB-owned or related content, or add language or commentary, to sell or to market UOB products or to provide financial advice on their personal pages and other social media channels including the Company's official social media channels. If you need materials to support the company's image for use on social media, please contact the Marketing or SCB function.

   b. Employees are not allowed to accept instructions from customers over Internet public forums or social media networks. You must move these conversations to bank monitored channels such as email or Microsoft Teams.

   **Examples:**
   - **Do** share an official post from UOB's Facebook page promoting a piece of media coverage from your own social media account.

   - **Do Not** add your own promotional line, comment, or opinion when sharing an official post from UOB's Facebook page promoting a new home loan offering, e.g. "I work in UOB and can confirm that this is a good home loan deal as it is much better than what the market currently offers!".

3. ***Personal opinions should be explicitly expressed as the Employee's own***

   a. Employees are allowed to indicate in their social media profile on professional social media sites such as LinkedIn, that they work for UOB. However, Employees should indicate their actual corporate titles and not misrepresent themselves. It should be noted that listing the Company name and job title on publicly accessible social media profiles, such as LinkedIn, carries the risk of the employee being targeted by social engineering attacks using the listed information.

   b. Employees should not share confidential information (e.g. budget, financial numbers, strategy, privileged accesses etc.) about their role or work in the Bank on their social media profile.

c. Employees should not comment or express personal opinion on matters related to UOB's stakeholders, competitors and industry. Beyond direct mention, this includes any form of indirect reference, allusion or association.

d. Employees may post articles or contribute to forums and discussion boards in their personal capacity on matters that do not relate directly or indirectly to UOB but they should clearly express that views are their own and not that of UOB. One way to do so is to include a line as part of their article or contribution, e.g. "These are my personal views and do not represent that of my employer.".

e. Employees should note that even with the above expressed clause, it may still be perceived that their views are representative of UOB's by virtue of their being an employee of the Bank. As such, Employees should be mindful of what they post online and be aware that they can be identified as an employee of UOB even if they do not mention UOB on their social media profiles or content posted.

**Examples:**

- **Do** list UOB as your employer on social media channels such as LinkedIn. However, please assume that all actions you take thereafter could be associated with UOB or be seen as being representative of UOB.

- **Do Not** comment on the misconduct of others, e.g. if the incident involves staff of a competitor. This could be perceived as self-righteous and not in line with UOB's values.

***4. Be respectful of colleagues, other individuals, the UOB workplace and communities***

a. Employees should be polite and respectful of others' opinions, be mindful of their behaviour online and ensure it is in line with the UOB values, policies and the UOB Code of Conduct.

b. Employees must respect the law and ensure that they do not post material that is or might be perceived as obscene, defamatory, threatening, harassing, discriminatory or hateful to another person or entity. Ethnic or religious slurs, personal insults and obscenities are unacceptable.

c. Employees should be respectful of their colleagues and refrain from commenting about them online. Personal social media accounts, blogs and websites must not be used to make comments about work, or to attack and abuse colleagues or UOB.

d. Permission from external parties like clients and business partners, and colleagues, both current and former, should be sought before posting any quote, photo or video of them, or tagging them. This includes members of management teams. If in doubt, do not post the content.

e. You are encouraged to discuss any issues, complaints or suggestions concerning your job or workplace to your supervisor and function head in accordance to our Collective Labor Agreement and not express them in public settings or online platforms.

f. Employees should be aware of and observe the terms and conditions of the social media platform used.

**Examples:**

- **Do** tag your fellow colleagues in photos of UOB Heartbeat Run/Walk after they have given you permission to do so, and only if the photos will be perceived positively.

- **Do Not** leave a negative complaint on a forum, calling out the name of the manager with whom you may have had disagreements.

## Non-Compliance

If an Employee fails to comply with this Protocol, he/she may face disciplinary action, up to and including termination of employment with UOB.

Misuse of social media websites and platforms could constitute an offence or give rise to certain legal liabilities under applicable law. Employees will be held personally liable for any such offence.

Employees are urged to exercise discretion in their actions in the digital space. Exercise good judgment when engaging online. Do not take risks with UOB's reputation or that of your own. UOB proactively monitors actions and conversations taking place in the digital and social space and reserves the right to restrict or to prevent access to websites or platforms deemed inappropriate.

Remember that as an employee of UOB, one must act in accordance with the highest standards of ethical and professional behaviour and in line with the requirements set out in the UOB Reputational Risk Management Policy, Social Media Policy, and Code of Conduct Banks and Bank Staff.

The online landscape and technology change very quickly and it is not possible to cover all possible scenarios and consequences in this document. This Protocol will be reviewed regularly to ensure that it stays relevant and applicable to new technologies, platforms and situations.

If you have questions on this Protocol and how it applies to you or discussion and clarification of any potential conflicts of interest, please contact the SMU in SCB and HR.

## 6.7 Proceedings

Unless prohibited by local laws, Employees must inform their supervisors, Human Resources and Legal immediately if they are the subject of the following:

- bankruptcy proceedings
- criminal prosecution or other criminal proceedings
- investigation by law enforcement agencies, or governmental or regulatory authorities
- civil proceedings if the proceedings impact the Employee's duties at UOB or have an adverse impact on UOB
- proceedings to disqualify the Employee from acting as a director of any corporation or from taking part, directly or indirectly, in the management of any corporation

Legal documents pertaining to the proceedings must be furnished to Legal immediately.

## 6.8 Political and External Activities

You must obtain approval before standing for political office or accepting any external employment, appointment or assignment.

### (A) Political Activity

UOB is politically neutral and has a longstanding policy of not making contributions to political parties or campaigns in all countries in which we operate. Employees wishing to run for political office or accept a political office must obtain prior approval from Human Resources. In addition, Employees are not allowed to use UOB's name, funds or resources in connection with any political campaign or purpose without first consulting Human Resources.

### (B) External Activities

Employees must obtain written approval (Appendix 5 of The Code) from their segment or function head before accepting any kind of external employment, appointment or assignment, or serving as a director, trustee, officer, owner, partner or consultant of a for-profit organisation, regardless of whether any form of compensation is received.

Employees volunteering to serve a non-profit organisation without any form of compensation should inform their supervisor. Any actual, potential or perceived conflict of interest should also be declared to the supervisor.

## 6.9 Anti-Competitive Practices

Employees should be mindful to not engage in business activities that may violate or cause the Bank to violate the Anti-Monopoly and Unfair Business Competition Law or any applicable competition or anti-trust laws or regulations. Employees should be mindful and identify the actions or types of business activities and practices that may raise competition law issues.

A particularly serious type of anti-competitive agreement would be those made by cartels, to divide up markets or to limit production. Cartels are competitors in the same industry who restrict competition by various means in agreement with one another. There are four main types of cartel agreements:

**(i) Price Fixing**

Price fixing involves competitors agreeing to fix, control or maintain the prices of goods or services. It can be 'direct' fixing of prices, where there is an agreement to increase or maintain actual prices. Price fixing activities can also take the form of 'indirect' fixing of prices, for example, where competitors agree to offer the same discounts or credit terms. Price fixing agreements do not have to be in writing, a verbal understanding at, for instance a trade association meeting or at a social event, may be sufficient to show that there was a price fixing agreement. It does not matter how the agreement was reached or whether it has been carried out. What matters is that the competitors have agreed to collude.

**(ii) Bid Rigging**

Bid rigging occurs when competitors agree on who should win a tender. To support the cartel member that has been designated to 'win' the tender bid, other cartel members may refrain from bidding, withdraw their bid, or submit bids with higher prices or unacceptable terms. The cartel members may agree amongst themselves to take turns to be the designated 'winner' or to reward 'supporters' of the winning bid, for example, by giving sub-contracts to them. As a result of bid rigging, the party inviting the tender is likely to pay more than it would if the tender was competitive.

**(iii) Market Sharing**

In a market sharing agreement, competitors divide up markets in various ways, such as geographical area or size or type of customer (e.g. business/non-business) and agree to sell only to their allotted segment of the market. As a result, they do not compete for each other's allotted market. Customers are affected as they would not be able to shop around for the best deals.

**(iv) Production Control**

Production control involves an agreement between competitors to limit the quantity of goods or services available in the market. By controlling the supply or production of goods or services, the cartel is able to, indirectly, increase prices to maximise their profits.

Competition in a market can be restricted in various other ways other than those set out above. For instance, there may be other types of agreements among competitors such as price guidelines or recommendations, joint purchasing or selling, setting technical or design standards, and agreement to share business information. If you require clarification on competition law issues, please contact Legal for assistance.

## 6.10 Anti–Money Laundering/Countering the Financing of Terrorism, Countering the Financing of the Proliferation of Weapons of Mass Destruction and Sanctions Controls

Employees must comply fully with applicable laws, regulations, policies, procedures and guidelines related to anti–money laundering (AML), countering the financing of terrorism (CFT), funding the proliferation of weapons of mass destruction and sanctions imposed by regulators. Adequate measures shall be taken to assess the legal, regulatory, and reputational risks associated with UOB business and undertake actions to prevent financial crime and illicit activities and ensure that UOB services are not used for the furtherance of any criminal or illegal purpose or activity (including tax evasion).

Employee is strictly prohibited from assisting, advising, or enabling customers or any third parties in any attempt to circumvent or undermine the Bank's AML/CFT and sanctions controls and requirements.

For further information on all Anti-Money Laundering, Counter-Terrorist Financing, Counter-Proliferation of Weapons of Mass Destruction and Sanctions Policies imposed by the regulator, please refer to Law of the Republic of Indonesia No. 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering and Law of the Republic of Indonesia No. 9 of 2013 concerning Prevention and Eradication of the Crime of Terrorism Financing regarding the Implementation of Programs as well as Policies and Procedures related to Anti-Money Laundering, Counter-Terrorist Financing, Counter-Proliferation of Weapons of Mass Destruction and Sanctions applicable to the Company.

## 6.11 Complying with Laws and Regulations

Employees are responsible for knowing and complying with the laws and regulations of the countries in which their businesses operate.

## 6.12 Non-Solicitation

During employment and for a period of six months following the termination of employment or such other period as may be stipulated in the employment contract (the "exclusion" period), an Employee must not directly or indirectly entice or induce another Employee to leave the employment of UOB or draw customers away from the Bank.

During the exclusion period, the Employee must not solicit business from any person, firm or corporation (the "entities") where:

- the entities have business dealings with the Bank; or
- the Employee had dealt with the entities in the six months before leaving the UOB's employment.

## 6.13 Agents, Consultants and Third Parties

Employees must exercise appropriate business judgment when selecting third-party Business Associates. This includes, but is not limited to, contractors, agents, agency staff, consultants, vendors and suppliers of goods and services. Such Business Associates

should not do that which an Employee is prohibited from doing under the Code or applicable laws and regulations.

Employees must conduct appropriate due diligence to ensure the following:

- the Business Associates are suitable for the task to be undertaken
- they have a good track record of ethical and professional conduct
- they do not exploit their relationship with UOB
- they do not use UOB's name in connection with any illegal, fraudulent, unethical or dishonest transaction, or any transaction that may sully UOB's reputation

For more information on selection and due diligence of vendors, refer to Finance and Corporate Services' Procurement and Payment Policy and Risk Management's Third-Party and Outsourcing Risk Management Policy available on the UOB Policy Portal in the intranet.

Employees must ensure that Business Associates are aware of and commit themselves to the anti-bribery principles set out in the Code and/or have similar anti-bribery compliance programmes in place.

**Q&A**

Q: A friend of mine from another financial institution informs me that one of his corporate clients is about to be acquired by a larger competitor. He suggests we buy some of the company's shares as the price is likely to go up and we should make a good profit. Would it be insider trading if I do so, as the company is not a client of UOB?

A: Yes, it would. The information is price-sensitive and if you trade using the information, you will be guilty of insider trading. It does not matter that the price-sensitive information is not related to a client of UOB.

**Q&A**

Q: I have been served a writ by the Court for my alleged involvement in insider trading at my previous company, even though I played no part in it. What should I do?

A: You must notify your manager and Human Resources and forward all legal documents right away.

**Q&A**

Q: I am a senior manager and a customer offers me a hamper with expensive items in it to thank me for a recent transaction I successfully completed. Can I accept it?

A: Since the transaction has already been completed, it does not appear that your business judgment will be improperly influenced by the hamper. However, the decision as to whether you can accept the hamper also depends on its value. If the value is S$150 or below, you may accept the hamper and do not have to disclose. If the value is more than this, you must complete a Declaration of Gifts form and submit it to Function Head or the Designated Officer appointed by the Function Head. The appointed employee by the Function Head then has the discretion to decide whether to let you keep the hamper.

**Q&A**

Q: Why do I have to inform my supervisor before accepting an offer to serve as a director for a non-profit organisation (NGO)? After all, I do this after working hours and it will not affect my work.

A: This is to avoid perceived or actual conflicts of interest and potentially adverse publicity should UOB have any engagement with the non-profit organisation – for instance, should the NGO become a customer of the Bank.

## CHAPTER 7 – WHISTLEBLOWING

*We have whistleblowing policy in place to provide you with an avenue to raise concerns. The identity of whistleblower and the information provided will be kept strictly confidential. Whistleblowers will be protected from reprisals or victimisation if the allegations are reported in good faith.*

We provide independent channels for you to report attempted or actual wrongdoing should you be aware of one. Examples of such wrongdoing include conflict of interest, corruption, fraud or possible violation of law, regulation, policy within UOB.

Personal work-related grievances, such as complaints on suboptimal physical working environment or perceived favouritism by supervisors, are generally not considered whistleblowing cases. You are encouraged to discuss such grievances to your supervisor and function head in accordance with our Collective Labor Agreement and not expressed them in the public or online platforms.

We will keep the identity and the information provided by the whistleblower strictly confidential except under exceptional circumstances as outlined in the Whistleblowing Policy. In such instances, we will make every reasonable effort to inform the whistleblower of the disclosure.

We will protect all whistleblowers, including those assisting in investigations, from any repercussions or victimisation, provided their reports are made in good faith. We will take disciplinary action against any employee who treats a whistleblower unfairly. We will also take disciplinary action against any employee who submits a frivolous or malicious report driven by personal gain or vendetta.

You can submit whistleblowing report throught one of the following independent channels:

1. ***Whistleblowing hotline***
   - Phone : (021) 2993-6679
   - Mobile (Call/WhatsApp) : (+62) 8121127222
   - Address : UOB Plaza 16th Floor
     Jl. M.H. Thamrin no.10, Jakarta 10230

2. **Whistleblowing Form** which can be downloaded from UOB Intranet, to be completed and sent to:
    - Email to whistle.blowing@uob.co.id
    - Postmail (marked “Private & Confidential”) addressed to:
        a) Head of Internal Audit UOB Indonesia
        UOB Plaza, 16th floor
        Jl. M. H. Thamrin no. 10, Jakarta 10230
        b) President Director; or
        c) Chairman of the Audit Committee UOB Indonesia
        UOB Plaza, 45th floor
        Jl. M. H. Thamrin no. 10, Jakarta 10230

**3. e-Whistleblowing form in UOB Website.**

## CHAPTER 8 – NON-COMPLIANCE WITH THE CODE OF CONDUCT

*Non-compliance with the Code will have serious consequences on the Bank. You are expected to comply with the law, regulations, the Code and UOB policies and standards. Violations will subject you to disciplinary actions.*

Non-compliance with the Code may expose the Bank to legal and regulatory repercussions, financial penalties, and reputational damage that can erode stakeholder trust. The impact of reputational risk extends beyond immediate consequences, including undermining our franchise, and diminishing investor and customer confidence. For more information on reputational risk, please refer to Risk Management Policy.

If you violate any laws, regulation, the Code or UOB policies and standards, you may be subject to disciplinary actions, including termination of employment. Ignorance of these requirements is not a valid excuse for non-compliance. For more information on employee disciplinary matters, please refer to the Employee Discipline Policy. We may report you to the relevant authorities for breaches of applicable laws or regulations, and we may take relevant legal actions against you, where appropriate.

Failure to report or promptly report a known or suspected violation may subject you to disciplinary action. We do not tolerate any form of retaliation against those who makes the violations allegations in good faith. Any attempt to do so may also subject you to disciplinary action.

## CHAPTER 9 – APPENDICES

### Appendix 1

### Declaration of Gifts

| | |
|---|---|
| *Name of Employee* | |
| *Employee number* | |
| *Employee segment, function, division, branch or subsidiary* | |
| *Name(s) of person(s) or organisation(s)* offering or receiving gifts* | |
| *Nature of relationship: Business Associate, customer or other* (please specify)* | |
| *Date(s) received* | |
| *Description of the gifts (include estimated value)* | |

*Delete where not applicable

_____
*Signature of Employee*
*Date:*

***Declaration verified by:***

_____
*Designated Officer*
*Date:*

***Declaration endorsed by:***

_____
*Segment/Function Head*
*Date:*

**Appendix 2**

**Declaration of Entertainment**

| | |
|---|---|
| *Name of Employee* | |
| *Employee number* | |
| *Employee segment, function, division, branch or subsidiary* | |
| *Name(s) of person(s) or organisation(s)* offering or receiving entertainment* | |
| *Nature of relationship: Business Associate, customer or other* (please specify)* | |
| *Date(s) received* | |
| *Description of the entertainment (include estimated value)* | |

*Delete where not applicable

_____
*Signature of Employee*
*Date:*

***Declaration verified by:***

_____
*Designated Officer*
*Date:*

***Declaration endorsed by:***

_____
*Segment/Function Head*
*Date:*

**Appendix 3**

**Gift Register**

| **No.** | **Name of Employee or recipient** | **Depart-ment** | **Description of gift received or offered** | **Value of gift** | **Name of giver of gift or person receiving gift** | **Relationship**, *such as Business Associate or customer* |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Appendix 4

## Entertainment Register

| **No.** | **Name of Employee or recipient** | **Depart-ment** | **Description of entertainment received or offered** | **Value of entertain-ment** | **Name of giver of entertain-ment or person receiving entertain-ment** | **Relationship**, *such as Business Associate or customer* |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Appendix 5**

**Declaration of Ownership and Management of Business/ Other Work**

To : *Name of Segment/Function Head*
Acknowledged: *Compliance, Legal and Corporate Secretary Director*
*Head of HR*
Subject : Business Ownership/ Occupation Information/ Other

I, the undersigned below:

Name of employee :
Employee number :
Position title :
Function :

declare that I own and/or manage the business/work _____ in _____ and that in terms of ownership and/or management of the business/work I:

☐ Earn income in any form, with the amount of _____ / annum
☐ Not earning any income in any form

I also ensure that the business/ work that I run does not violate The Code of PT Bank UOB Indonesia and will not affect my work and responsibilities as an Employee of PT Bank UOB Indonesia.

If I am proven to have done things that are contrary to the provisions of the Company, then I am willing to receive sanctions in accordance with applicable provisions.

_____
*Signature of Employee*
*Date:*

## Appendix 6

## Illegal or Unethical Business Conduct Red Flags

(i) Poor Reputation

- Party has a poor business reputation or a reputation for unethical conduct, including reports of suspicious, unethical, or unlawful conduct about the party, its sub-agents or its employees.
- Party has a history of improper payment practices, such as prior or ongoing formal or informal investigations by law enforcement authorities or prior convictions.
- Party has been subject to criminal enforcement actions or civil actions for acts suggesting illegal, improper or unethical conduct.
- Allegations the party has made or has a propensity to make prohibited payments or facilitation payments to officials.
- Allegations related to integrity, such as a reputation for illegal, improper, or unethical conduct.
- Party does not have in place an adequate compliance program or code of conduct or refuses to adopt one.
- Other companies have terminated the party for improper conduct.

(ii) Ties to Government and Public Officials

(iii) Questionable or Unusual Circumstances

- Lack of written agreement or refusal to execute a written agreement or requests to perform services without a written agreement where one is sought.
- Misrepresentation or inconsistencies in the party's application or during the due diligence process.
- Failure to cooperate with the due diligence investigation or refusal to answer questions or make representations and warranties.
- Refusal to accept audit clauses in contracts.
- Requests for anonymity or insistence that the identity remain confidential or that the relationship remain secret.
- Refusal to divulge the identity of beneficial owners, directors, officers, or other principals.

(iv) Unusual Compensation and Questionable Accounting or Invoicing

- Excessive or unusually high compensation.
- Fee, commission, or volume discount provided is unusually high compared to market rate.
- Compensation arrangement is based on a success fee or bonus; unusual bonuses for foreign operating managers.
- Requests for a commission or other payment substantially above the market rate or a substantial up-front payment or unusual advance payment.
- Request to share compensation with others whose identities are not disclosed.
- Request for increase in compensation during sales or marketing campaign or at period end.

(v) Insufficient Capabilities

- Party lacks the staff, facilities, or expertise to perform substantial work.
- Party lacks relevant industry/technical experience or a "track record" with the product, service, field or industry.
- Party has not been in business for very long or was only recently incorporated.
- Party is in a different line of business than that for which it has been engaged.
- Party has an unorthodox corporate structure.
- Party's business address is a mail drop location, virtual office, or small private office that could not hold a business the size that is claimed.

- Party has poor financial statements or credit.

Such indicators must be evaluated to understand any actual risks, any reasonable resolution or measures which must be implemented to mitigate a risk, or if UOB should not engage the third party because the risk is unacceptable.