krungsri
กรุงศรี

A member of MUFG
a global financial group



THE SPIRIT & THE LETTER

ปรัชญาและสำนึกในการปฏิบัติงาน

- REGULATORY EXELLENCE
- WORKING WITH CUSTOMERS & SUPPLIERS
- WORKING WITH GOVERNMENTS
- COMPLYING WITH COMPETITION LAWS
- IN THE KRUNGSRI COMMUNITY
- PROTECTING KRUNGSRI ASSETS

Call 1572 | www.krungsri.com | Krungsri Simple

Contents

3 Message from CEO

4 The Spirit & The Letter

6 Krungsri Code of Conduct

8 Your Personal Commitment

9 Who must follow The Spirit & The Letter

10 What employees must do

11 What leaders must do

13 Raise Your Voice: Your obligation to raise integrity concerns.

14 How to Raise an Integrity Concern?

15 What happens when an integrity concern is raised?

16 Penalties for violations

Corporate policies and procedures

17 The Spirit & The Letter Policies

18 01 Regulatory Excellence

20 Regulatory Excellence

22 02 Working with Customers & Suppliers

24 Improper Payments

27 Supplier Relationships

30 Sanctions Compliance

31 Money Laundering Prevention

34 Privacy

36 03 Working with Governments

38 Working with Governments

40 04 Complying with Competition Laws

42 Complying with Competition Laws

44 05 In the Krungsri Community

46 Fair Employment Practices

48 Environment, Health & Safety

51 Security & Crisis management

54 06 Protecting Krungsri Assets

56 Intellectual Property

58 Controllership

62 Conflict of Interest

64 Handling of Material Non-Public Information (MNPI) and Preventing Insider Trading

Message from CEO

The Spirit & The Letter of our Bank is built on honesty, integrity, and good corporate governance. These principles from the foundation of our transparent business practices and accountability, which are essential for sustainable growth.

To ensure compliance with the Bank's "The Spirit & The Letter", every employee must adhere to both the letter and the spirit of the law and the Bank's policies. This means not only following the rules but also embracing their underlying principles. Such conduct safeguards our reputation and maintains customer confidence, driving sustainable growth.

Krungsri staff are committed to achieving a Zero Non-Compliance target, reinforcing our ambition to be the Leading Sustainable and Regional Bank. Integrity and good governance are indispensable for our success.

Yours sincerely,

Chief Executive Officer



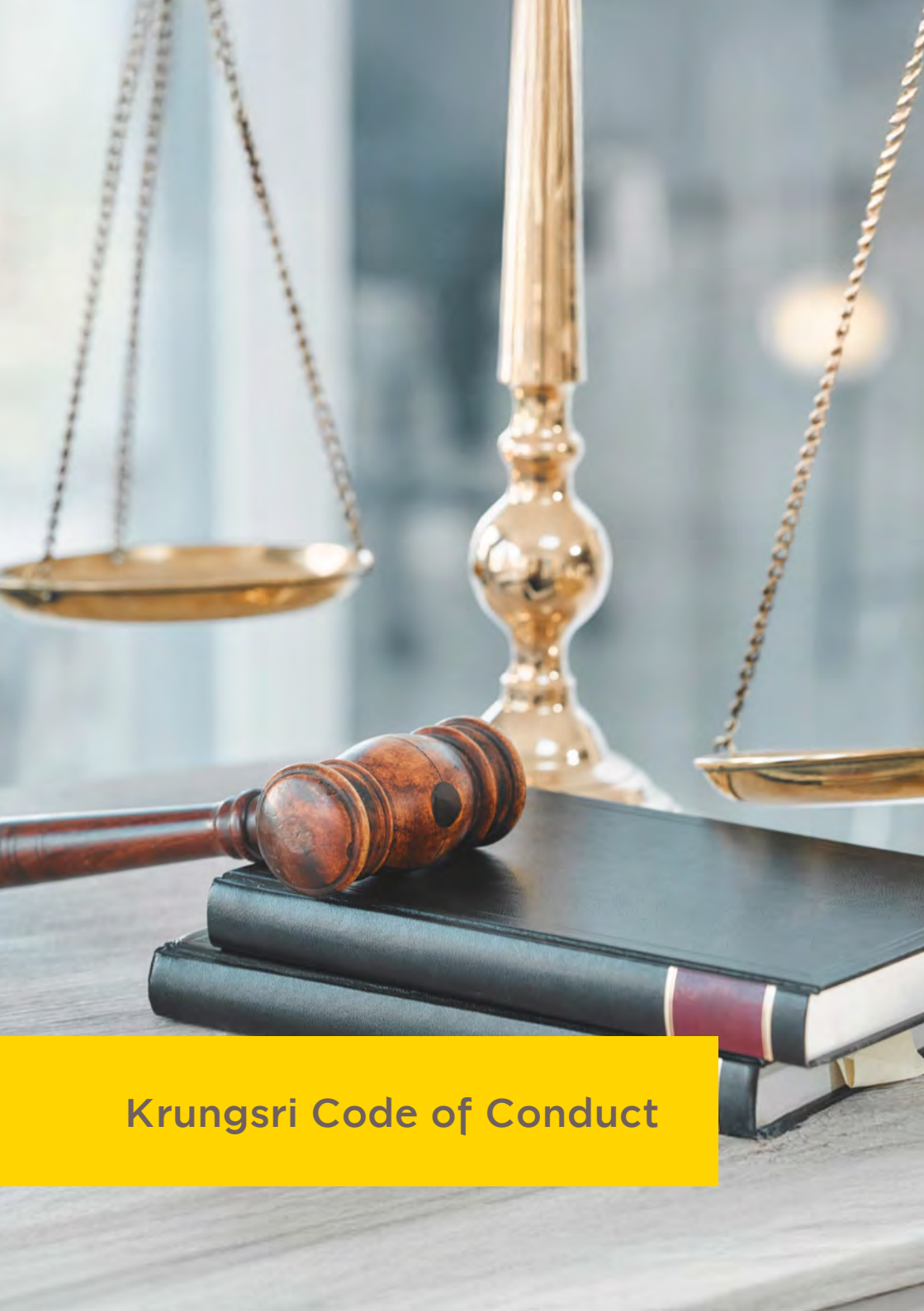
The Spirit & The Letter



The conduct of all employees may have an impact on the Bank's reputation. Employee must conduct in compliance with ***The Spirit and The Letter*** which helps to ensure that we perform duties and conduct banking business with integrity.

All employees also have the responsibility to uphold the highest standards of ethical business conduct. We prioritize not only conduct in compliance with the written requirements of the law but also adherence to the spirit of integrity.

The spirit of honesty is used as a guideline for determining the practice as reflected in the Bank's Code of Conduct that all employees must apply everywhere and every day.



Krungsri Code of Conduct



Compliance with laws and regulations governing our business.

- Be honest, fair and trustworthy in any activities and relationships related to the Bank.
- Avoid all conflicts of interest between work and personal affairs.
- Promote a fair employment for all members of the Bank's diverse community.
- Strive to create a safe workplace and to protect the environment.
- Leaders, at all levels, shall sustain a working culture where ethical conduct is recognized, valued and exemplified by all employees.

Your Personal Commitment

All employees must understand and comply with the Bank's Code of Conduct throughout their employment with the Bank.

Employees acknowledge the policies and procedures that have been communicated to them, which will act as their guidelines while working at the Bank. Supervisors must provide employees with the necessary knowledge and information about these guidelines and ensure they are adhered to. Violation of the Bank's policies and procedures will result in disciplinary action, possibly including termination.

You will be asked to acknowledge your awareness that all employees of the Bank must follow to the Bank's Code of Conduct and Policies and raise concerns about possible violations of law or policy with your supervisor, ombudsperson or Compliance Group.

You can read the complete and up-to-date policies at **onekrungsriportal.net.** The Code of Conduct outlined here cannot encompass every situation. It is the responsibility of all employees to use personal judgment carefully to determine the correct way to resolve the situations they face.

The following questions should be considered to decide about taking any action.

1. Whether the actions taken are align with moral, laws and the Bank's procedure.
2. Whether the action enhance the image of integrity for both the individual and the Bank.
3. Whether the action is socially acceptable and can be openly disclosed.
4. Whether the action be perceived as indicating 'inappropriate' behavior.

Who must follow The Spirit & The Letter

Directors, Executive Officers and All Employees of the Bank

Companies in Financial Business Group of the Bank

Companies in the financial business group, which the Bank holds 50 percent or more of shares or has control over such company, are required to comply with policies and procedures of the Bank.

Companies in the financial business group, which the Bank holds less than 50 percent of shares or has no control over such company, should be encouraged to comply with Code of Conduct and compliance related policies of the Bank.

Third parties representing the Bank

Bank employees working with third parties, such as consultants, agents, sales representatives, distributors and independent contractors, must:

- Require these third parties to agree to comply with relevant aspects of the Bank's policies and procedures.
- Provide these parties with education and information about policy's requirements.
- Take extreme actions, which may include a termination of a hiring contract, after learning that a third party failed to abide by the Bank's policies and procedures.

What employees must do

All employees can contribute to the Bank's compliance culture with policies and regulations by understanding the Bank's policies, conduct in compliance with the Bank's integrity and acting to enforce compliance with policies and regulations and avoid violations.

Employee responsibilities are as follows:

Understand the Bank's Policies

- Understand the basic requirements of the policies summarized in this book.
- Learn the details of the policies related to your job.
- For any inquiries about the policies, consult your supervisor or the Policy and Procedure owner.

Raise Your Concerns

- Promptly raise any suspected potential violations of the Bank's policies.
- Study various channels for reporting integrity concerns, such as supervisor, ombudsperson or Compliance Group.
- If a concern raised is not resolved, please continue to report it through other channels within the Bank.
- Collaborate in the investigation related to integrity concerns.

What leaders must do



A supervisor must establish a compliance culture to conduct in compliance with policies and regulations , promote ethical and compliance behavior via being a role model, include compliance factor in employee performance evaluation.

A supervisor must create a framework to prevent, detect and handle compliance issues with policies and regulations by the following steps.

Prevent Compliance Issues

- Identify business risks if not conduct in compliance with policies and regulations.
- Ensure that processes tailored to address particular risk areas, are communicated to all employees and implemented.
- Provide education on the Bank's policies and applicable law to employees and board members and third parties.
- Allocate adequate resources to conduct in compliance with policies and regulations.

Detect Compliance Issues

- Implement control measures, such as "dashboard" and "scorecards," to detect heightened compliance risks and/or violations of policies and regulations.
- Promote an effective whistleblowing system.
- Ensure that periodic compliance reviews on complying with policies and regulations are conducted, with the assistance of Compliance Champions and/or the Internal Audit Group.

Handle Compliance Issues

- Take prompt corrective action to fix identified policy and regulatory compliance deficiencies.
- Take appropriate disciplinary action.
- Consult with Chief Compliance Officer and make appropriate information disclosures to regulators and law enforcement authorities.

Raise Your Voice: Your obligation to raise integrity concerns

Raising an integrity concern protects the Bank's community which is composed of the Bank, colleagues and stakeholders.

If you have any concerns about complying with Krungsri policies, you have a duty to report such concerns.

Raise Concern Early

The longer you wait to address a concern, the severe it may become.

Whistleblowers or complainants may choose to remain anonymous.

However, if they disclose their identity, we can follow up and give them feedback.

Information Confidentiality Is Respected

The names of whistleblowers or complainants and the details they provide will only be revealed when 'necessary' to those responsible for resolving the issue.

Obstructing investigation is a violation of the Bank's policy.

The Bank prohibits any interference with investigations or actions that make complainants, whistleblowers, or those cooperating in the investigation feel they are being treated unfairly.

Obstructing an investigation will result in the highest disciplinary action, which may include termination.

How to Raise an Integrity Concern?

The Bank has provided several channels for raising concerns. Please use the one that is most convenient for you.

Within Your Business Unit

Generally, your supervisor is in the best position to swiftly resolve an integrity concern. However, you can choose to raise your concerns to your supervisor or the following alternatives:

- The next level supervisor whom the whistleblower or complainant trusts.
- Compliance Group (Head of Governance Compliance Department)
- The ombudsperson, appointed by the President and CEO, there are 3 channels as follows:
  1. Telephone
     1.1 For Head Office: Tel. 85588
     1.2 For Branch: Tel. 02 296 5588
  2. Mail: P.O. Box 169 Yan Nawa Bangkok 10120
  3. Krungsri Portal -> Compliance -> Ombuds Corner
- Branch Compliance: Tel. 83456 press 1 and then press 2
- HR Group: HR Hotline Tel. 85577
- Audit Committee: there are 2 channels as follows:
  1. E-mail: audit.committee@krungsri.com
  2. Mail: Audit Committee, Bank of Ayudhya Plc, 1222 Rama III Road, Bang Phongphang, Yan Nawa, Bangkok 10120

- MUFG Channel (English or Japanese language only): send via mail or email.

1. **Nishimura & Asahi Law Firm**
   Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo, 100-8124, Japan
   email: mufgwhistleblow@nishimura.com

2. **MUFG Audit Committee**
   JP-Tower, 2-7-2, Marunouchi, Chiyoda-ku, Tokyo, 100-0005, Japan
   email: mufg-group-helpline_kansaiinkai_PF@mufg.jp

Ombudsperson

Ombudsperson process allows you to voice your integrity questions and concerns, you may choose anonymously and your issues shall be handle.

What happens when an integrity concern is raised?

Concerns about compliance with Krungsri policy will be investigated per the following processes.

1. **Appoint an investigation committee**
   Appoint experts with appropriate knowledge and fairness to conduct a fact-finding investigation.

2. **Investigation**
   The committee will gather and determine the facts based on interviews and/or document review.

3. **Corrective action**
   If necessary, the committee will recommend corrective actions for relevant staff to implement.

4. **Investigation result**
   Investigation result shall be notified to the person who raises the concern. (If an identity is disclosed.)

Penalties for violations

Employees and supervisors who violate the Bank's policies, whether in spirit or in letter, will be subject to the highest disciplinary actions, potential termination. Conduct that may lead to disciplinary action includes:

- Violating the Bank's policies.
- Persuading or requesting others to violate Krungsri' policies.
- Failing to report violations of the Bank's policies immediately.
- Not cooperating in investigations of potential the Bank's policy violations.
- Obstructing an investigation or persecuting towards employees who report integrity suspicions which can result in unfair treatment.
- Failing to demonstrate leadership and efforts to comply with laws and the Bank's policies."

Corporate policies and procedures

Your business may have its own policies and procedures. You must comply with such policies and procedures in addition to those mentioned in this guide.



The Spirit & The Letter Policies

- Regulatory Excellence
- Working with Customers & Suppliers
- Working with Governments
- Complying with Competition Laws
- In the Krungsri Community
- Protecting Krungsri Assets



01

Regulatory Excellence

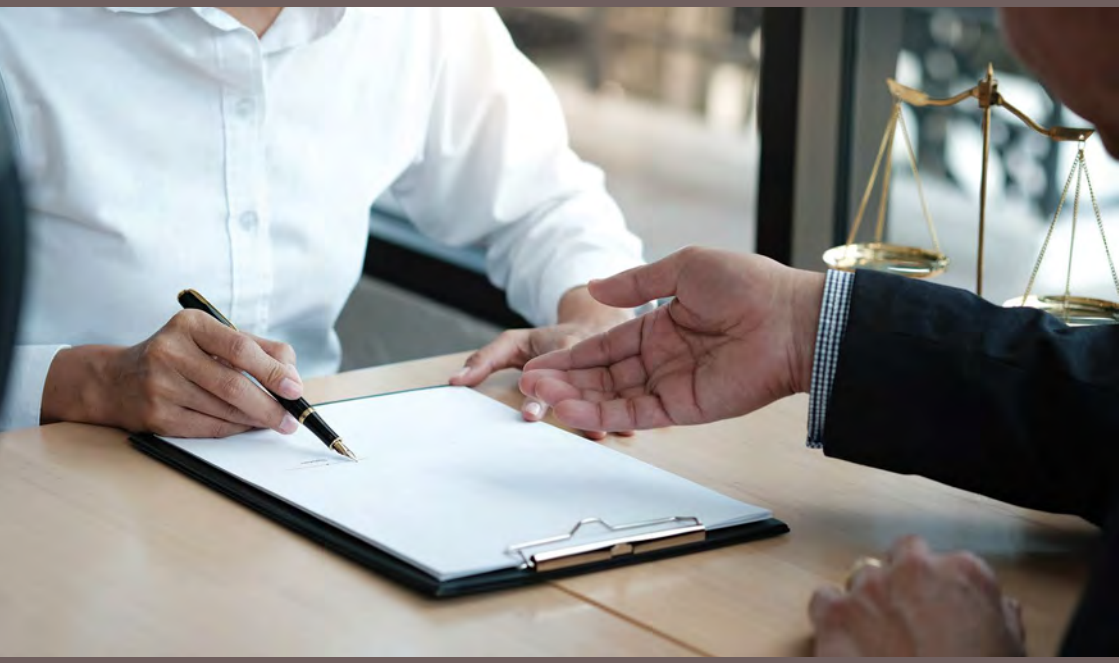


The policies in The Spirit & The Letter are formulated based on laws and regulations issued by government authorities that oversee banking business. These regulations affect all businesses and employees of the Bank. Regulatory authorities establish rules that we must comply with in our business operations.

Therefore, cooperating with these regulatory authorities in issuing such regulations and strictly adhering to them is a crucial factor in maintaining the Bank's reputation.

Currently, laws and regulations are becoming more challenging for practitioners. The Banks must conduct business under an increasing number of laws and regulations. Therefore, all employees and executives must be aware of and knowledgeable about these regulations and strive for excellence in compliance.

Regulatory Excellence



Responsibilities of all employees

- Be knowledgeable about and comply with policies mentioned in The Spirit & The Letter that affect your job.
- Be aware of the specific regulatory requirements that affect your job.
- Have a basic understanding of regulators and their priorities that affect your job.
- Report any concerns or issues that may lead to regulatory violations immediately.
- Always treat regulators professionally with courtesy and respect.
- Assure that you coordinate with the Bank's designated departments or contact persons when working with or responding to requests of regulators.

Responsibilities of Executive Managements

Executives have the following additional responsibilities for regulatory compliance:

Leadership

- Assure that you and your staff comply with policies and regulatory requirements and manage non-compliance risk properly.
- Embed regulatory requirements into operating processes and procedures.

Human Resource

- Designate employees to handle regulatory compliance risks and ensure they coordinate with the Bank's assigned regulatory contacts.
- Manage to ensure the department has experts who can effectively manage compliance practices.

Anticipation

- Implement effective work processes that provide new/change regulatory enforcement alert, especially those related to work.

Relationship

- Develop and maintain good relationships with regulators.
- Work proactively with regulators to develop various regulations.

Control

- Control operations and conduct audit to assess the effectiveness of compliance practices.



02

Working with Customers & Suppliers



The Bank employee is invited by a customer to attend a seminar held outside Bangkok. The customer is responsible for all expenses throughout the trip such as accommodation, meals, and travel expenses.

In this scenario, do you think such employee can attend this seminar?

Please see the following page for guidance on Anti-Bribery and Corruption to acknowledge precautions and proper action before conducting activities between the Bank, business partners, government officials or other persons.

Your supplier offers good quality and reliable delivery at lowest prices that can't be beaten. But you are uncomfortable with the working and living conditions it provides to its workers.

Shrug it off, or make an issue of it?

SEE PAGE: 27 SUPPLIER RELATIONSHIPS

Improper Payments

What To know

An improper payment to gain advantage in any situation is never acceptable and exposes you and Krungsri to possible criminal prosecution. Krungsri expressly prohibits improper payments in all business dealings, in every location, with both governments and private sector.

Anti-bribery and corruption is one of the Bank's crucial missions in conducting business in accordance with good ethical principles. Executives and employees are prohibited from being involved in or aware of bribery and corruption in any form, even if it may provide business opportunities. The Executives and employees shall not be illegally exploited for the benefit of one's own or others through abusive use of assets, information or position held in the bank.

Therefore, the Bank has established policies and operating procedures related to anti-bribery and corruption to guide the Executives, employees and companies in the Bank's financial business group strictly follow the rules.

Bribery and Corruption

"Bribery" is the offering, promising or delivery of anything other of monetary value. Either directly or indirectly, with the aim of obtaining or retaining a business or business advantage that is not transparent.

"Corruption" is the abuse of entrusted power or state power for private gain or others. This includes bribery of government officials or any other act that falls under the category of other criminal offenses to obtain unlawful benefits.

ANSWER TO QUESTION ON PAGE 23

You should consult your supervisor or contact Financial Crimes Compliance Advisory and Testing Department to determine whether customer shall provide the expense for the seminar trip is acceptable. Since we must consider many factors which include whether the customer is a public official, as well as considering the Bank's policies, and any other relevant issues.

What to do

The employees are not allowed to perform the following prohibited activities:

1. Giving or receiving cash/cash equivalents, except in the case of giving cash for funerals, weddings and Buddhist ordination, which can be given by cheque issued in the name of the Bank.
2. Giving or receiving anything of value, whether directly or indirectly, to customers, third parties, public officials, or others. This includes the cost of gifts, hospitality services, and other expenses, etc.
3. Giving facilitation payment to public officials.
4. Falsifying or concealing any books, records, accounts, or other information in relation to the bank's activities, customers, service providers, suppliers, counter parties or business partners of the Bank.
5. Violating any relevant laws, regulations, or the Bank's policies and procedures.
6. Making political contributions with the Bank's funds or on behalf of the Bank, to improperly influence any external party in connection with the Bank's business, or in exchange for any improper business advantage.

Therefore, when giving/receiving anything of value to/from customers, third party, public officials, or others, please refer to the provisions of the Bank's policies and procedures, and laws related to anti-bribery and corruption.

What to watch out for

Employees must ensure that their actions comply with the laws and the Bank's policies or procedures, avoiding conflicts of interest that may lead to bribery and corruption risks or legal offenses.

Principles for consideration and review include:

1. For a legitimate business purpose, such as:
    - 1.1. Connected to the establishment or maintenance of business relationships, or the promotion, demonstration, or explanation of Bank products or services.
    - 1.2. Never improperly obtain or retain business or other business advantages or create an image that may cause the damage to the Bank.

2 Reasonable based on the facts and circumstances, including but not limited to:

2.1. The nature of the business relationship between the provider and recipient.

2.2. The proximity to new, recently completed, or expected business or government action.

2.3. The type, cost/value, and setting of what is given (i.e., whether it is lavish or too frequent in relation to the recipient).

2.4. Whether the recipients are public officials may cause a conflict of interest situation.

3 Accurately and completely recorded in the Bank's books and records.

Considering the background information of individuals who represent the Bank or may be selected as representatives of the Bank, which indicates.

- Allegations of improper business practices.
- Reputation for bribes.
- Family or other relationship that could improperly influence the decision of a customer or government official.
- Any demand to receive a commission payment before the announcement of an award decision.
- Any suggestion to acquire business for the Bank through a specific representative or partner due to "special relationship".
- Any request to make a payment in other country or to a person who is not related to the transaction.
- A commission that is disproportionate to the services provided.

Supplier Relationships



What to know

The relationships between the Bank and suppliers are based on lawful, efficient and fair practices. We expect our suppliers to obey the laws that require them to treat workers fairly, provide a safe and healthy work environment and protect environment. Following Krungsri guidelines ensure that our supplier relationships will not damage the Bank's reputation.

ANSWER TO QUESTION ON PAGE 23

Do not shrug it off. It's a big issue and may impact our reputation. We shall do business with suppliers that have responsibility to their workers and their local environment only.

What to do

Comply with Applicable Laws and government regulations related to supplier relationships.

- Do business only with suppliers that comply with applicable legal requirements and the Bank's guidelines relating to labor, the environment, health and safety.
- Provide a competitive opportunity for suppliers to earn a share of the Bank's business volume, including small businesses and businesses owned by the disadvantaged, minorities, women and disable veterans.
- Safeguard the Bank's confidential and proprietary information with a confidentiality agreement and safeguard any supplier-provided information protected by any confidentiality agreement.
- Safeguard of "personal data" obtained from suppliers (for instructions, see "Privacy" on page 34

What to watch out for

- Choosing suppliers on any basis other than open, competitive bidding.
- Potential conflicts of interest in supplier selection, such as accepting improper gifts or other items of value.
- Directing business to a supplier owned or managed by a relative or close friend.
- Unsafe conditions in supplier facilities.
- Supplier employees who appear to be underage or subject to coercion.
- Apparent disregard of environmental standards in supplier facilities.
- Entrusting "personal data" or confidential information to suppliers without ensuring that they have appropriate technical, physical, and organizational measures to prevent unauthorized access or use.

A major deposit customer of a branch frequently deposits and withdraws more than 2 million baht in cash each time. However, these transactions are divided into multiple withdrawals, each less than 2 million baht. The branch staff considered this behavior normal due to the customer's significance and did not find it suspicious.

Is it appropriate for the branch staff not to examine these transactions and consider reporting them as suspicious transactions?

Please refer to page 31 for guidance on Money Laundering Prevention.



A representative from a potential new customer or supplier has given you his name card, containing his name and contact details.

Is it OK to put this information in a database where any Bank's staff can access it?

SEE PAGE: 34 PRIVACY



Sanctions Compliance

What to know

The Bank is obligated to adhere to sanctions laws and regulations (Sanctions measures), including the Bank's policies and procedures. Sanctions measures are imposed by the United Nations Security Council (UNSC) of United Nations (UN), the Office Foreign Assets Control (OFAC) of U.S. Treasury Department, Japan Ministry of Finance (JMOF).

According to the sanction's measures, individuals and organizations who subjected to sanctions shall be prohibited from engaging in any financial transactions or providing financial supports or services to individuals, organizations, or activities that are sanctioned. Non-compliance with these measures poses significant compliance risks and may result in legal action.

What to do

The Bank has established policies and procedures to abide by sanctions measures, including terminating of customer relationships, refraining from offering products/services, refraining from facilitating any transactions, both directly and indirectly, or engaging with individuals, entities, countries, or territories subjected to sanctions.

According to the sanction's measures, individuals and organizations who subjected to sanctions shall be prohibited from engaging in any financial transactions or providing financial supports or services to individuals, organizations, or activities that are sanctioned. Non-compliance with these measures poses significant compliance risks and may result in legal action.

What to watch out for

Customers being uncooperative, falsifying information, or providing false information when establishing a relationship or conducting a transaction requires contacting the Financial Crimes Compliance Division before proceeding.

Money Laundering Prevention

What to know

The Bank is obligated to adhere to the Anti-Money Laundering Act B.E. 2542 and Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559, along with other relevant laws to prevent the Bank from being exploited for illicit activities.

To achieve these objectives, the Bank has implemented relevant policies, procedures, and manuals, such as Procedure for Know Your Customer/ Customer Due Diligence (KYC/CDD), Procedure for Operating Procedure Process of Anti-Money Laundering and Combating Financing of Terrorism, etc. These materials are in place to support operations and prevent the money laundering and terrorist financing (AML/CFT) risks that could occur.

Additionally, the Bank has a committee and executives responsible for overseeing AML/CFT risks ensuring the effectiveness of organization risk management.

?

ANSWER TO QUESTION ON PAGE 29

Our AML law requires reporting cash transaction valued THB 2 million and up and any person of integrity will follow the law. Avoidance of following the law is red flag of a suspicious activity.

What to do

In the operations such as the establishment of relationships with customers, supplier, correspondent banking, and other involved parties, as well as other activities, executives and employees shall ensure compliance with the Bank's policies and procedures related to AML/CFT.

When establishing relations or conducting transactions with customers, suppliers, correspondent banking, and other involved parties, it is necessary to perform KYC/CDD, including proceed name screening against the AML Watch List database. In case of any parties' name matched with the designated person or blocked person categories, the staff shall strictly adhere to the Bank's policies, procedures, and manuals.

Furthermore, according to the Anti-Money Laundering Office (AMLO)'s requirements, any units involved in reporting transactions to the AMLO shall be responsible for preparing and/or submitting (where applicable) the reports within a specific timeframe. In cases where suspicious activity is identified, it requires contacting the Financial Crimes Compliance Division for investigating and reporting suspicious transactions to executives and AMLO.



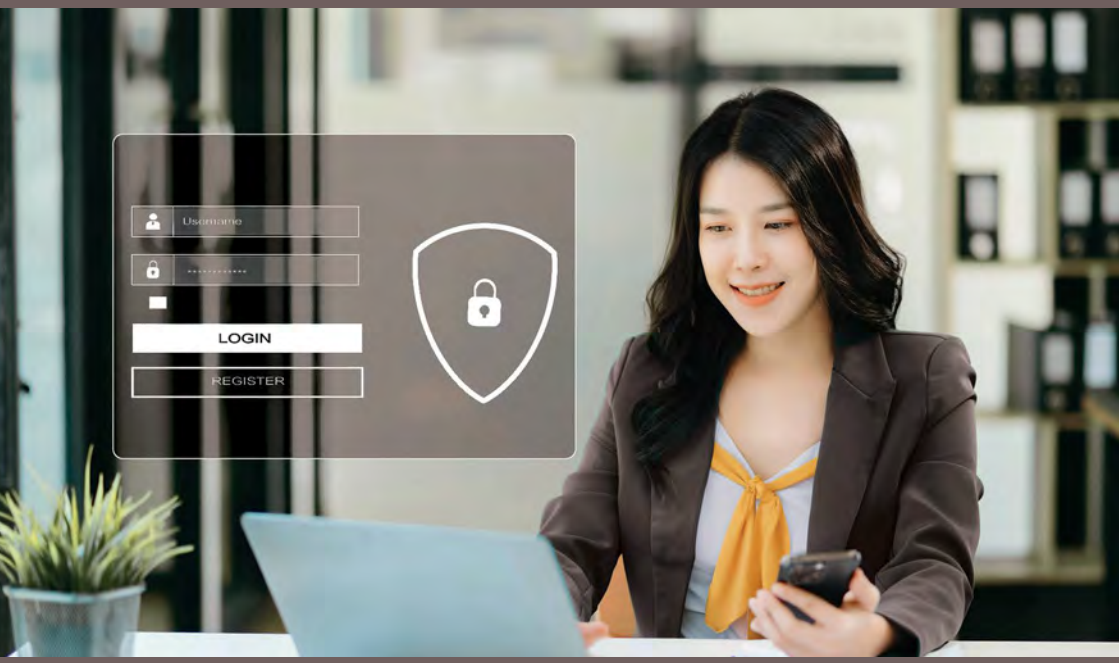
What to watch out for

The Bank shall not establish relationships or conduct transactions with customers, suppliers , correspondent banking, and/or other parties demonstrating the following behaviors:

1. Individuals who conceal their true names or use false names or aliases for identification.
2. Those providing inadequate/incorrect information, refusing cooperation, or attempting to impede KYC/CDD process.
3. Payments made with financial instruments lacking clear connections to the customers.
4. Transactions with counterparties residing in high-risk countries lacking substantial supporting information.
5. Transactions involved terrorism, drug trafficking, or money laundering.
6. Transactions involving shell banks, offshore banks, unlicensed money transfer or money exchange service providers, or non-bank financial intermediaries.
7. Any structuring of transactions to avoid transaction reporting requirements (e.g., multiple transactions below the reporting threshold).
8. Any financial transaction provides to the customers which cannot obtain or identify the relationship, the purpose of the transaction and/or the source of fund.

These behaviors are identified as red flags related to AML/CFT risks. Therefore, if anyone found such activities, please contact the Financial Crimes Compliance Division for further investigation.

Privacy



What to know

A growing number of countries are more stringently regulating the collection, use, and disclosure of consumers' "personal data" (names, home and office contact information and other data). In addition, many countries regulate personal data of company representatives. Some countries even regulate the privacy of information relating to juristic persons. corporations. Krungsri employees should realizes the importance of personal data and shall uphold the privacy and security of personal data to ensure that such personal data is collected, used, or disclosed in compliance with the laws.

ANSWER TO QUESTION ON PAGE 29

No, since proper access control shall be applied.

What to do

Learn and comply with the followings personal data related regulations:

- Applicable laws and regulations regarding the collection, use, or disclosure (process) of personal data.
- The Policy for Personal Data Protection.
- Related contractual obligations.
  - Process personal data for legitimate righteous business purposes.
  - Prevent any personal data breach.

If you know that there is a personal data breach or deficiency of security measures of any system or device containing personal data, immediately notify your supervisor, or Compliance Group.

What to watch out for

E-mailing personal data to a larger group of recipients, beyond need to know basis, or leaving document with personal data at a printer, copy machine or fax machine may disclose data to others.

Sharing of personal data to third parties, who lack appropriate security safeguards or restrictions on information use.

Transfers of personal data between countries, regardless of applicable legal requirements.



03

Working with Governments



You propose a complex risk management product to a customer who is a government agency. You know other banks also offer similar products to the customer. Once the customer agrees to buy our product, you immediately sign the contract.

Is it OK to urgently sign the contract even before ensuring the customer fully understands the risk associated with the products and can enter the contract?

SEE PAGE: 38 WORKING WITH GOVERNMENTS

Working with Governments



What to know

To conduct banking business with governments and government-owned enterprises, either directly or indirectly, we frequently interact with government agencies and officials. In any circumstance, Krungsri employees must apply the highest ethical standards and comply with applicable laws and regulations, including certain special requirements associated with government transactions.

What to do

Abide by applicable laws and regulations relating to working with governments, particularly special requirements associated with government contracts and transactions.

Require parties who works with the Bank on financial contracts for government projects (i.e. a company investing in the project, a company working in the project, a financial consulting company) to abide by the spirit of the Bank's Working with Governments policy.

Be truthful and accurate when dealing with government officials and agencies.

Proceed to ensure that reports, certification, statements and proposals reflect current, correct and completed status, also requirements are adequately identified and communicated with the responsible parties.

Do not make any unauthorized changes or deviate from contract requirements without the written approval of the authorized government official.

What to watch out for

- Special requirements on business transactions with governments, including commercial transactions with private parties financed by government agencies or international agencies.
- Charging fees/expenses which are incorrected or not align with contract.
- Deviations from contract requirements, i.e. allowing withdrawal of fund prior to the completion of a task as specified in the contract.
- Violating government regulations on gratuity or gift or bidding procedures.
- Accepting legitimate government suppliers' selection information or competitors' bid or proposal.
- Hiring negotiation of family members of government officials or government officials who influence decision making on contracts with the Bank and the government.



04

Complying with Competition Laws



Complying with Competition Laws



What to know

The Bank commits to transparently operating our business. Not only strengthen transparent working culture, but we also expand this to related societies and communities.

Our competition framework intends to prevent unfair competition. The Bank's staff must comprehend the fundamental requirements of relevant law, policies and procedures to prevent illegal supporting to customers.

What to do

- Studying competition law, business practices, including reviewing and comprehending relevant the Bank's procedures.
- Customers' behavior related to competition laws violations shall be factored in for granting loans to such customers.
- **Do not facilitate** a customer who intends to use our service as a vehicle to avoid competition laws; for example, using our letter of guarantee to bid a government project but not intend to win the bid or just to make the bidding appeared to be non-transparent, using our fund to facilitate unlawful merger or acquisition or to facilitate market activities which will result in monopolizing the market or evading anti-dumping law.
- Avoid any contact with competitors that could create the appearance of improper agreements or understandings.
- Do not facilitate customers or suppliers who do not intend to use our facilitation for their own use (in other words, customers or suppliers who are nominees of unknown persons).

What to watch out for

If the customer or suppliers receives an appointment contract as Distributor or agent Sole trade, broker, licensee or licensor to produce/distribute/using product or service, we must ensure that such customer or business partner does not violate competition law.



05

In the Krungsri Community



Fair Employment Practices

What to know

Fair employment practices are not only for the Bank to comply with applicable labor and employment laws but also promote a culture of respect. The Bank is committed to complying with any laws pertaining to freedom of association, privacy, wages and working hours, including no employment discrimination.

What to do

- **Base employment decisions** on qualifications (e.g. education and experience) and appropriateness which means an individual's skills, performance, values, leadership and other job-related criteria.
- **Make all employment related decisions and actions** regardless of race, color, religion, sex (including pregnancy), sexual orientation, age, disability, veteran status or other characteristic protected by law.
- **Provide a work environment** without harassment and bullying.
- **Respect privacy rights** of employees by collecting, using or disclosing personal data appropriately. However, Krungsri reserves the right to monitor use of the Bank's property, including computers, e-mail, phones, proprietary information.
- **If a conflict arises** between the requirements of fair employment and laws, or practices, the consultation with Executives and Legal Group Head shall be taken to determine the most appropriate course of action.

What to watch out for

- **A hostile work environment** occurs when one's behavior within a workplace causes an environment that is difficult or uncomfortable for another person to work in.
- **Treating employees or co-workers** of the opposite sex inappropriately.
- **Refusing to work** or cooperate with certain individuals because of their race, religion, sex or other characteristics protected by law.
- **Disclosing employment data** to a person who does not need to know or has no authority or without a consent from an employee.
- **Violating a labor law.**
- **Taking an adverse action** against an employee (e.g. threatening, no promotion) because such employee has raised a concern about a violation of policy or law.

A department places 50 boxes containing documents to be delivered to warehouse for record keeping in the next few days. The boxes are placed along a walkway and take up some space of fire-exit.

Should you place those boxes there?

SEE PAGE: 48 ENVIRONMENT, HEALTH & SAFETY



Environment, Health & Safety



What to know

Protecting environment, health and safety of employees is mentioned in law and it is the right thing to do. The Bank commits to provide safe workplaces, not only for staff safety but also for customers and or anyone who enters our workplaces. This policy affects all activities of the Bank not just within the Bank's workplaces, but everything we do for example, acquiring a new business or providing customer service.

ANSWER TO QUESTION ON PAGE 47

No, blocking the walkway of the fire exit would be considered as an unsafe working environment. Thus, do not place any article blocking the fire exit.

What to do

- Comply with all applicable environmental health and safety (EHS) laws and regulations and EHS policies of the Bank.
- Create and maintain a safe working environment and prevent workplace injuries.
- Assess EHS legal and reputational risks before acquiring a new business.
- Consider EHS impacts as a credit criterion – take into account that if a customer violates EHS law and regulations, it may impact its ability to repay our loan and impact our reputation as a company that does not concern EHS.
- Eliminate inappropriate EHS risks from facilities, products, services and activities of the Bank.
- As practicable, reduce toxic and hazardous materials, prevent pollution, conserve, recover and recycle materials, water and energy.
- Continue to improve our EHS systems and performance as an integral part of the Bank's operational strategy.
- Present ideas that support the goals of this policy to your manager or your business's EHS manager.
- Promptly alert your manager or EHS contact of unlawful or unsafe conditions.

What to watch out for

Unsafe activities and conditions, such as

- Exposed or unsafe wiring.
- Blocked fire or emergency exits.
- Working on electrical or powered equipment without conducting in compliance with safety procedures.
- Potential exposure to serious infectious diseases.
- Disabling safety control or protective guarding equipment and machinery.

Failure to comply with health, safety or environmental regulations and procedures.

EHS complaints or unreported hazards/ accidents or ignorance to environmental, health or safety issues, including safety related to customer's business operation should be taken into account as a potential to our operating risk and reputational risk.

Inadequate security procedures or practices that may present safety threats to a facility and/ or employees.

New business acquisitions that may increase or lead to credit and reputational risks to the Bank.

Security & Crisis management



What to know

Protecting the security of our people, workplaces, information and business is critical. This starts with all business unit implementing Security and Crisis Management (SCM) plan which includes measures for preventing terrorist and other criminal acts on our employees, workplace, information, information technology (IT) infrastructure, business continuity and crisis management. In addition, employees must take every precaution to avoid doing business with known terrorists or those known to support terrorist activity.

What to do

- Implement rigorous plans to address the security of employees, facilities, information, IT assets and business continuity.
- Participate in contingency plan and contingency drills.
- Comply with the entry and exit rules at the Bank's premises, including wearing the appropriate badge.
- Protect access to the Bank's premises from unauthorized personnel.
- Protect the Bank's assets from theft or misappropriation.
- Create and maintain a safe working environment – this includes identifying and reporting indicators of workplace incidents.
- Conduct appropriate background checks on new hires and contractors, wherever allowed by law.
- Ensure proper business continuity plans for an emergency.
- Screen all customers, suppliers, agents, dealers and business partners against appropriate terrorist watch lists.
- Report any apparent security lapses to your manager, crisis management leader or Ombudsperson of the Bank.

What to watch out for

- Individuals not wearing appropriate badges and loitering in our premises.
- Unsecure IT assets such as laptop, servers, etc.
- Secured premises where only authorized personnel allowed to enter.
- Security complaints from employees, customers or neighbors.
- Unauthorized entry to premises.
- Conducting business with customers , suppliers or any third parties without sufficient checking.





06

Protecting Krungsri Assets

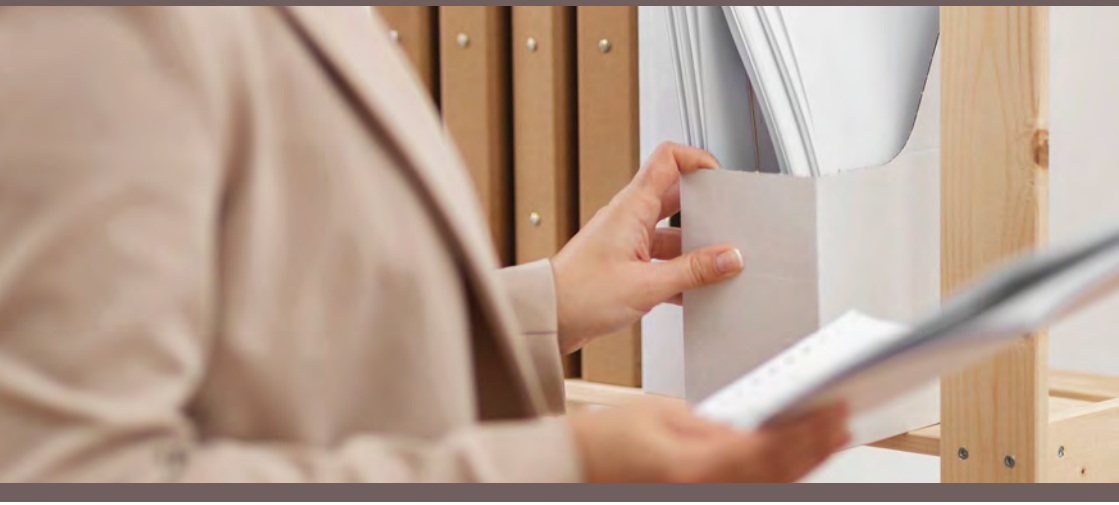


Consumer banking has internally revealed an innovative financial instrument. A big customer of mine is pressing me to describe the new instrument to her now because she needs to make her decision this week. I know the Bank wants to protect the feature but I'm not sure the application has been filed yet.

Can I show the customer the new product?

SEE PAGE: 56 INTELLECTUAL PROPERTY

Intellectual Property



What to know

Intellectual property of the Bank is one of its most valuable assets. All employees must try to safeguard patents, trademarks, copyrights, trade secrets and other proprietary information of the Bank. At the same time, it is critical that **we respect intellectual property rights of others.** Unauthorized use of other's intellectual property can expose the Bank and employees to civil lawsuits and damages, including significant fines and criminal penalties. A key to protecting our intellectual property and, at the same time, guarding against these risks, is periodically review of new Krungsri products, services, processes and software, for possible inventions and trade secrets, including infringement of intellectual property rights of others.

ANSWER TO QUESTION ON PAGE 55

No. You should consult with your manager if the product has gone through internal approval process as well as regulatory process and reach the stage that you could release it to a customer.

What to do

- Protect our logo using of our logo and name of the Bank shall be reviewed by Legal Group and Compliance Group.
- Do not use intellectual property of the Bank for personal affairs or activities.
- Respect valid patents, copyright and other protected intellectual property of others.
- Consult with Legal Group concerning necessary licenses or approvals to use protected intellectual property of others such as patents, trademarks.
- Allow third parties to use intellectual property of the Bank. (In case the Bank requests the organization or a third party to use the logo of the Bank, please discuss with relevant business unit.)
- Learn about your responsibilities to the Bank regarding its intellectual property, trademarks and trade names.
- Comply with the guidelines for using logo and trade names of the Bank and our Financial Business Group.

What to watch out for

- Using information belonging to an outsider without prior consultation with Legal Group and Compliance Group.
- Having another company develop new products or software without a written agreement covering ownership and other rights for the developed intellectual property.
- Threatening suspect for infringing any intellectual property of the Bank without prior consultation with Legal Group.
- Hiring an employee, especially one who previously worked for a competitor, without preventive measures to prevent such employee from inadvertently disclosing or using the proprietary information of the previous employer.

Controllership

What to know

Controllership embodies three fundamental elements: (1) principles that categorize transactions and balances appropriately; (2) systems and controls that protect assets and accumulate information consistently and correctly; and (3) financial and transaction reporting that is timely and unbiased. Controllership creates the right environment for disclosing timely, reliable, and accurate information to government agencies and public.

What to do

- Follow Group Accounting Guidance for financial reporting to comply with the Conceptual Framework for Financial Reporting issued by the Federation of Accounting Professions and regulations by the Bank of Thailand, and/or other regulatory requirements.
- Ensure that financial and non-financial information and operating metrics are reported accurately and in a timely manner.
- Maintain accurate and complete accounting records to appropriately reflect all business transactions.
- Safeguard all company assets both physical assets and information.
- Provide forecasts and review consistently.
- Maintain appropriate processes and controls.
- Complying with established document management procedures as well as all applicable laws and regulations relating to the retention of documents and records.
- Maintain documents and records relevant to pending or reasonably foreseeable litigation, audits or investigation, as directed by Legal Group and Lawsuit and NPA Division of the Bank.

What to watch out for

- Financial reports that do not reflect actual performance.
- Inaccurate bookings records, such as overstated travel expense, or incorrect invoices.
- Transactions that are inconsistent with good business economics.
- Lack of controls to protect assets from risk of losses.
- Avoidance of review and approval procedures.
- Inadequate procedure and controls to retain documents (including e-mail) for pending or reasonably foreseeable litigation for audit and investigations.
- Documents destruction without knowing what is being discarded or whether the documents are subject to legal preservation requirements.
- False or exaggerated statements in e-mail, presentations or other documents.





I was chatting with my brother and informed him that I was in the process of reviewing the information to sign a contract for Krungsri to acquire Company X.

Could this create a problem?

SEE PAGE: 64 Handling Material Non-Public Information (MNPI) and Preventing Insider Trading



Your cousin owns a company that supplies office equipment to the Bank.

Is this a prohibited conflict of interest?

SEE PAGE: 62 CONFLICT OF INTEREST

Conflict of Interest

What to know

On the job or in our free time, nothing you do shall conflict with your responsibilities to the Bank. No activity at work or at home should damage the Bank's reputation or good name. Misusing the Bank resources or influence is also prohibited. Even without bad intention, the appearance of a conflict can have negative effects. It is crucial to consider how your actions might appear, and to avoid the perception of a conflict of interest.

ANSWER TO QUESTION ON PAGE 61

Conflict of Interest policy requires that you disclose the situation to supervisor and Core Compliance Division. Also, you do must not attempt to influence the Bank's business process with your cousin's company.

What to do

- Declare (in written form to your supervisor and Core Compliance Division) all your outside activities, financial interests or relationships that may either present a conflict or the appearance of one.
- Use good judgment in all personal and business dealings.
- Avoid actions or relationships that may cause conflict or create the appearance of a conflict with your job or the Bank's interests.
- Do not misuse/use Krungsri resources, intellectual property, office hours, or the Bank's facilities for personal gain, including office equipment, e-mail and computer applications.
- Do not take any advantage from opportunity or information collected while being employed by the Bank for personal gain.
- Get your supervisor's approval before taking on the role, responsibility or position in other organization, either profit or non-profit ones. Especially, those which has any relationship with the Bank or may anticipate support from the Bank while the employee is still employed.

What to watch out for

- Financial Interests in a company which causes business impact to the Bank (for example, a customer, supplier or investment).
- Part-time Jobs performed during the Bank's business hours or using the Bank's equipment or materials.
- High value gifts from suppliers, customers or competitors, particularly when you participate in decision making (on the Bank's behalf) that involve them.
- Personally obtaining discount or other benefits from suppliers, service providers or customers that normal people or other employees do not obtain.
- Directing Business to suppliers when you know they are owned or misusing the Bank's resources such as your position or influence to promote or assist an outside activity.
- Hiring, Promoting or directly supervising a family member or close friend.
- Personal relationships that may conflict with roles and responsibilities for the Bank or compromise the Bank interests.

Handling of Material Non-Public Information (MNPI) and Preventing Insider Trading

What to know

In the course of your job, you may obtain material information about the Bank or other companies before it is made public. You may be the Relationship Manager of a client or may simply overhear a hallway conversation or come across a memo left at a copy machine. Using this information for your financial or other personal benefit or conveying this information to others constitutes a violation of this policy and may even violate the law. This includes buying or selling the securities of any company which you have material non-public information and giving this "inside information" to anyone else who might base financial trades on the information you've shared.

ANSWER TO QUESTION ON PAGE 60

Yes, if Company X is a public company and the possible acquisition of Company X has not been publicly announced. If your brother trades Company X stock based on your tip, both of you could be charged with insider trading.

What to do

Do not buy or sell securities of any company, including the Bank, either directly or through family members or other persons or entities, while you are aware of inside information about the company or the Bank. (This is known as "insider trading.")

Do not recommend or suggest anyone to buy or sell securities of any company, including the Bank, while you have inside information about the company or the Bank. (This is known as "tipping.")

Maintain the Confidentiality of the Bank information and do not convey information to anyone.

If questions Arise, consult Governance Compliance Department before trading securities or disclosing the Bank information.

What to watch out for

Non-public information which, if disclosed, would certainly affect the price of a security or would influence your decision to buy, sell or hold a security, such as earnings announcement or a prospective acquisition announcement. (This is known as "inside information".)

Buying or selling securities because you hear or obtain information at work that you think will make the price go up or down once it's publicly announced.

Engaging in trading activity around the time of a significant the Bank announcement.

Discussing the Bank Krungsri business with family and friends.

Talking about what you're working on or places where you are travelling to work for the Bank or visitors of the Bank.



Visit **onekrungsriportal.net**
for the complete and up-to-date policies.