Handling of Confidential Information and Dealings in Securities

Principles of Best Practice

Singapore Exchange

Issued together with

abs The Association of Banks in Singapore

ISCA Institute of Singapore Chartered Accountants

The Law Society of Singapore

SID Singapore Institute of Directors

Contents

Introduction

1 SGX, together with the Association of Banks in Singapore, the Institute of Singapore Chartered Accountants, the Law Society of Singapore and the Singapore Institute of Directors, developed this guide to assist issuers and their advisers (e.g. lawyers, accountants and other professionals) in developing and implementing best practices in handling confidential information and dealings in securities. This guide aims to enhance public confidence in the Singapore capital markets by recommending practices that would ensure equal access of information by the market and orderly release of information when necessary. Issuers and their advisers are encouraged to adopt or adapt this guide according to the needs and complexities of their business.

2 Issuers deal with confidential information on a daily basis. The Listing Rules require issuers to immediately disclose material information. One of the necessary conditions under the Listing Rules to withhold the disclosure of material information that is not ready for disclosure is that the information is kept confidential[1]. For the purpose of this guide, such information shall be referred as "confidential information". Access to such confidential information should be restricted, to the extent possible, to the highest possible levels of management and should be disclosed to officers, employees and others only on a need-to-know basis. Distribution of related paperwork and other data should also be kept to a minimum.

3 Under the Securities and Futures Act (Cap. 289) ("SFA"), it is an offence if a corporation fails to prevent or detect market misconduct (including insider trading) by its employees and officers where the contravention has been committed for the benefit of the corporation and is attributable to the negligence of the corporation[2]. In addition, the Listing Rules require issuers to provide details of its internal compliance policy on dealing by the company and its officers in its securities. "Inside information", in this guide, refers to information concerning a corporation that is not generally available but, if the information were generally available, a reasonable person would expect it to have a material effect on the price or value of securities of that corporation.

4 The objectives of this guide are as follows:

- assisting issuers and their advisers in ensuring that confidential information generated and/or received by issuers and their advisers remains confidential until it is reasonably expected to be disclosed under the relevant laws, regulations and the Listing Rules;
- minimising the risks of accidental leakage of confidential information;
- preventing insider trading through effective trading restrictions on dealings in securities; and
- establishing strong consciousness of the importance of appropriate handling and control of confidential information.

5 This guide outlines principles and guidelines for issuers and their advisers in (i) creating a culture of compliance; (ii) handling and controlling confidential information; and (iii) restricting dealings in securities. It also includes practical examples on how issuers and their advisers can put these principles and guidelines into practice.

6 The principles set out the objectives to be achieved, while the guidelines and examples constitute leading practices to be followed. The guidelines and examples are not meant to be prescriptive, and companies may consider alternatives to achieving these objectives.

[1] *Rule 703(3) of the Listing Manual.*

[2] *Section 236C of the SFA.*

7 In addition, this guide should be tailored to the company's specific profile and circumstances. We recognize that for certain companies, the guidelines and examples may not be practically feasible. For example, for smaller sized companies which have budget constraints, automated surveillance systems or pre-dealing approvals in respect of securities of other listed companies may not be necessary. In other instances, the guidelines and examples may be more relevant for larger companies, financial institutions, or service providers which manage or undertake investments in multiple listed securities. Organisations are encouraged to exercise their own judgment when adopting the best practices in this guide.

8 This guide lays the groundwork in improving practices for the handling of confidential information and dealings in securities and helps issuers and their advisers fulfill their applicable statutory and listing obligations. It is in the interests of issuers and their advisers to implement robust policies and procedures to protect information and prevent insider trading.

December 2017

PART A

Creating A Culture Of Compliance

Principle A1

Have in place clear written policies and procedures on the handling of confidential information and restrictions on dealings in securities

Internal Compliance Policy

9 Organisations should adopt an internal compliance policy which provides guidance in non-legalistic language on the legal and regulatory prohibitions with regard to dealings in securities. The internal compliance policy should also set out the company's policies and employees' obligations regarding the handling, protection and disclosure of confidential information. The legal and regulatory prohibitions include, but are not limited to:

- statutory prohibitions against insider trading contained in Sections 218 and 219 of the SFA;
- statutory prohibitions against false trading and market rigging, securities market manipulation, making false or misleading statements contained in Sections 197, 198 and 199 of the SFA;
- statutory prohibitions against fraudulently inducing persons to deal in capital markets products, employing manipulative and deceptive devices, and disseminating information about illegal transactions contained in Sections 200, 201 and 202 of the SFA;
- Rule 703(4)(a) of the Listing Rules, under which issuers are required to comply with the Exchange's corporate disclosure policy, including obligations on issuers to ensure awareness and establish effective procedures for the prevention of improper trading; and
- Rule 1207(19) of the Listing Rules, which requires each issuer to disclose in its annual report a statement on whether and how it has complied with specific best practices on dealings in securities.

10 The internal compliance policy should be written in plain language in an easy to read manner. It may be contained in one or multiple policy documents. In particular:

- the scope of information and types of securities covered under the internal compliance policy, and persons to whom the internal compliance policy applies, should be clearly stated;
- it should be stressed that the prohibitions against insider trading and market misconduct are absolute, and not a matter of guidance;
- the potential civil and criminal sanctions which could result from a breach of obligations should be highlighted; and
- the internal compliance policy should be tailored to the organisation concerned. For example, if the organisation has multiple listed subsidiaries, associated companies or suppliers and contractors, the internal compliance policy should set out and explain requirements about dealing in those types of securities that the organisation considers appropriate.

11 As a matter of best practice, the internal compliance policy should be effective in preventing employees from dealing in securities, including through proxies. Companies may consider if it is appropriate to include dependents or immediate family members of employees in the policy. The internal compliance policy can require staff to notify such proxies of the insider dealing policy or can issue clear warnings to staff not to communicate confidential information to dependents and other third parties.

12 The examples below detail (i) the types of securities and scope of persons covered, and (ii) a description of "inside information" in the internal staff dealing policy of Company A.

Example

Company A is a listed property developer headquartered in Singapore with subsidiaries in Indonesia, the Philippines, Malaysia and Thailand (together, the "Group"). It has an Internal Policy for Dealings in Securities ("Staff Dealing Policy"). Securities covered under the Staff Dealing Policy are the securities of all Group companies ("Group Securities") and the policy has been drawn up with reference to the rules and regulations in Singapore, Indonesia, the Philippines, Malaysia and Thailand.

Persons covered under the Staff Dealing Policy include all senior management, executive officers, other employees and company secretaries of the Group ("Relevant Persons"), and immediate family members of Relevant Persons.

All Relevant Persons are provided with a copy of the Staff Dealing Policy as part of their induction process, and each such person are obliged under the Staff Dealing Policy to ensure that they and their immediate family members will comply with the Staff Dealing Policy.

Under the Staff Dealing Policy, several business units, senior management and specified Relevant Persons have been identified as being more likely to have access to confidential information in the course of their work. The dealing restrictions under the Staff Dealing Policy for these individuals are stricter as compared with other Relevant Persons, and could include near-complete prohibitions against in dealing in the Group Securities.

In general, Relevant Persons are urged to err on the side of caution, to not trade if they are in doubt as to its legality, and to seek legal advice when they are unsure.

Example

Company A's Staff Dealing Policy states that "inside information" refers to information relating to the Company or Group which is not generally available, but which a reasonable person would, if the information were generally available, expect it to have a material effect on the price or value of the Group Securities; and that a reasonable person would be taken to expect information to have a material effect on the price or value of Group Securities if the information would, or would be likely to, influence persons who commonly invest in securities in deciding whether or not to subscribe for, buy or sell the Group Securities.

Company A's Staff Dealing Policy also provides examples of possible inside information, which include but are not limited to:

- Proposed material acquisitions, sales, divestments, mergers, or takeovers of the Company or Group's assets, businesses or business units
- Financial information such as changes to profit results, earnings and dividends
- Restructuring plans
- Proposed material legal proceedings to be initiated by or against the Company or Group
- Investment or development decisions or plans
- Proposals to undertake a new issue of securities or major changes in financing
- Major supply and contractor agreements
- Changes in key management
- Asset revaluations

Written policies for investigations of breaches and enforcement actions

13 It is good practice for issuers and advisers to have written policies and procedures on (i) how a suspected breach of internal systems, processes and infrastructure is to be investigated, and (ii) what enforcement actions may be taken against wrongdoers, including guidelines for whether such breaches should be referred to the relevant authorities. Employees should be made aware of such policies and procedures. It is also good practice for companies to develop whistleblowing policies that make it easy for employees to report instances of inappropriate handling of confidential information.

Example

Company A's whistleblowing policy provides a dedicated email inbox and hotline for reporting irregularities where all complaints, whether named or anonymous, will be investigated. The Policy covers misappropriation of documents containing confidential information and failure to comply with laws, regulations and company policies. It assures employees that all concerns or irregularities raised will be treated with confidence and may be reported to the authorities and regulators where necessary.

Process to monitor trading activities

14 It is good practice for issuers to set in place processes to monitor share prices and volumes. One such process may be to use manual and/or automated surveillance systems. Issuers and advisers should pay close attention to trading activity that is unusual when compared to historical price or volume movements during periods where there are no corporate announcements. Issuers may also wish to monitor market and industry news on a continual basis. During price-sensitive or major transactions, both issuers and advisers should monitor the share prices and volumes for unusual activity.

15 As stated in Appendix 7.1 of the Listing Manual, when issuers identify periods of unusual trading activity, the issuer should consider whether any information about its affairs, which would account for the activity, has recently been publicly disclosed, whether there is any material information that has not been publicly disclosed (in which case, the unusual trading activity may signify that a "leak" has occurred), and whether the issuer is the subject of a rumour or report. The issuer should respond promptly to any enquiries made by the Exchange concerning the unusual trading activity and may be guided by the following:—

- If the issuer determines that the unusual trading activity results from material information that has been publicly disseminated via SGXNET, generally no further announcement is required. However, if the market activity indicates that such information may have been misinterpreted, it may be helpful, after discussion with the Exchange, to issue an announcement to clarify the matter;
- If the unusual trading activity results from the "leak" of material information, the information in question must be announced promptly. If the unusual trading activity results from a false rumour or report, the Exchange's policy on correction of such rumours and reports, (as discussed in "Clarification or Confirmation of Rumours or Reports" in Appendix 7.1 of the Listing Manual) should be observed; and
- If the issuer is unable to determine the cause of the unusual trading activity, the Exchange may suggest that the issuer makes a public announcement to the effect that there have been no undisclosed recent developments affecting the issuer or its affairs which would account for the unusual trading activity.

Example

Company A actively monitors its share price movements and volume traded, compared to its usual price movements and trading volumes. It relies on information services providers like data vendors to be alerted when prices or volumes hit threshold levels. This is especially so during key milestones in a transaction.

When Company A is engaging in a major asset acquisition, it monitors share prices even more closely with its advisers, to identify any unusual price movements. The issuer can also monitor market / industry news to better ascertain if the unusual price movements are attributable to leakage of confidential information or other external market developments.

Principle A2

Put in place measures to create a strong culture of awareness within the organisation of the risks of information flow and restrictions against dealings in securities

16 Organisations should aim to create a culture of awareness of the restrictions and internal compliance policy in relation to the handling of confidential information and dealings in securities. Some ways in which this can be done include:

- Setting a clear tone at the top with senior management leading by example
- Having a clear line of accountability
- Raising the profile of the internal compliance policy
- Establishing regular training and assessment of employees
- Incorporating compliance into everyday duties and performance reviews
- Imposing serious enforcement actions for breaches
- Placing effective technology in place

Taking a top-down approach with senior management leading by example

17 It is crucial for senior management to get on board by fully supporting and overseeing the company's compliance efforts. When senior management advocate the importance of the internal compliance policy, they send a clear message to the entire organisation that the company takes the protection of confidential information and restrictions on dealings in securities seriously. This has a direct impact in shaping organisational culture. Senior management should lead by example by complying with, and upholding a workplace environment which implements and is aligned with principles in the company's internal compliance policies. Where possible, senior management should also present, or at least be involved in, compliance training sessions.

Example

Company A's senior management and board of directors support and are closely involved with the company's compliance program. Each year, Company A's board exercises close oversight and approves the Company's overall internal compliance policy, including the compliance budget and compliance processes. At town halls and speeches, the senior management of Company A regularly endorse the compliance program, emphasising to all staff that compliance with internal compliance policies on the handling of confidential information and dealings in securities is important and will be enforced strictly.

Having a clear line of accountability

18 Having a clear line of accountability with senior management and independent committees helping to provide checks and balances is important. Listed issuers' audit committees and risk management/ compliance teams should be included in the line of reporting.

Example

Company A is a global multinational company with a dedicated Compliance team reporting directly to the CEO. A member of the Compliance team is specifically in charge of overseeing the Company's internal compliance policy in respect of the handling of confidential information and dealings in securities.

During each quarterly board session, the Compliance team updates the Board and Audit Committee of the functioning of the internal compliance policy. In particular, any breaches of restrictions regarding dealings in securities are reported.

There are clear channels of communication two-ways, between both (i) the Compliance Officer and unit or team heads; as well as (ii) the Compliance Officer and Audit Committee and Board. The firm's whistleblowing policy also allows individual employees to report concerns or complaints directly to t

19 It is good practice for the organisation to designate specific person(s) to oversee the development and implementation of policies and practices, and compliance with applicable laws and regulations relating to the handling of confidential information and dealings in securities across the company. This would include organising training for employees and ensuring that the internal compliance policy is communicated to all relevant persons.

Example

Company A, which is a multinational company, has designated a Compliance Officer to be responsible for the compliance with the Company's internal policy for the handling of confidential information and dealings in securities. The Compliance Officer reports directly to the Head of Compliance. The duties of the Compliance Officer include:

- Developing the Company's policy in relation to the handling of confidential information and dealings in securities (the "Policy")
- Overseeing the Company's training program in relation to the Policy
- Monitoring adherence to laws and regulations regarding dealings in securities, including coordinating internal and external audits of staff, transactions and units
- Conducting regular reviews of whether the Policy is working effectively in practice
- Ensuring that the Policy is regularly refreshed and updated
- Providing quarterly updates to the Board and Audit Committee
- Acting as the contact point to provide advice in cases of uncertainty

Raising the profile of the company's policy regarding dealings in securities

20 Employees at all levels should be made aware of the internal compliance policy. The internal compliance policy should be publicised in internal communications on a regular basis. As for external communications, organisations may also wish to publicly disclose e.g. on its website, that it has an internal compliance policy in place for the handling of confidential information and dealings in securities.

Example

Company A distributes written guidelines to all staff, setting out prohibitions against dealings in the Company's securities (i) while in possession of confidential information; and (ii) during restricted periods prior to and up to the time of announcement of the Company's interim and full year financial results. In addition, annual reminders on the Company's internal compliance policies regarding dealings in securities are sent to staff by email. Staffs are required to acknowledge compliance with the Company's internal compliance policy on dealings in securities by email on an annual basis. Reminders are also posted on the Company's Intranet, and include warnings against the use of any confidential information with respect to other companies or entities obtained in the course of employment.

21 The company's internal communications should be sufficiently clear and detailed to ensure that relevant parties understand the restrictions/ obligations imposed on them.

Example

Before the announcement of Company A's financial results, Company A sends out an organisation-wide email to all staff to remind them that there will be a black-out period for dealing in the Company's shares. The email reminder states that the employee and his/her immediate family members should not deal in the Company's securities within a specified time period (stating the start and end dates). The email reiterates the prohibition against insider trading and warns staff not to deal in the Company's securities while in possession of any confidential information in relation to the Company's securities (including outside the black-out period), or on short term considerations. Lastly, the email provides contact details for staff to contact a member of the compliance team if they have any questions.

Establishing regular training and assessment of employees

22 Staff training can be adapted for the training needs of employees (e.g. based on business functions, levels of experience, or extent of dealing with confidential information). The objective of the staff training should be for all employees to understand their obligations in respect of the handling of confidential information and dealings in securities, and to abide by the internal compliance policy when carrying out their day-to-day functions.

Example

Company A conducts e-learning on its Staff Dealing Policy every year. The e-learning module contains a refresher of the key concepts in the Staff Dealing Policy, and ends with a quiz containing scenario-based questions which staff will have to pass to successfully complete the module.

Company A has also identified certain business units which may come into possession of confidential information on a regular basis. These include the business deals (acquisition) team, the finance unit, human resources unit and senior management. For these identified units and staff, face-to-face training is conducted in addition to the company-wide e-learning. The training includes topics such as dealing with advisers, consultants, and third-parties, the handling of media queries, and the protection of confidential information in unit-specific scenarios (e.g. at different stages of the deal process; before the declaration of dividends and financial results; senior management appointments and cessation of service). The identified units and staff are also assessed on their awareness of the Company's internal compliance policy and Staff Dealing Policy on an annual basis through multiple choice and short-answer questions.

Incorporating compliance into everyday duties and performance reviews

23 As far as possible, staff should be encouraged to uphold good practices which are in line with the company's internal compliance policy for the handling of confidential information and dealings in securities. Whilst the company can implement procedures such as black-out periods or pre-dealing approvals (elaborated further in Principles C1 and C2), practical steps can also be taken at the individual unit level to protect the flow of confidential information and to ensure that team members are kept aware of the restrictions against dealings in securities.

Example

For each new transaction which involves potentially confidential information, a senior employee working on the transaction will be tasked to complete and maintain a privy persons list, setting out the persons in the transaction deal team who will be privy to information about the deal on a need-to-know basis. The same employee informs the Compliance team of the privy persons list, for the purposes of maintaining the Company's "restricted list" and "watch list". The senior employee is tasked with ensuring that arrangements are in place for third parties, advisers and professionals working on the deal to comply with their relevant confidentiality obligations/ undertakings in respect of dealing in the Company's securities.

24 Adherence with the internal compliance policy can be built into performance reviews to keep staff cognisant of their obligations in respect of the handling of confidential information and dealings in securities. For example, it could be a requirement for all staff to complete and pass an online e-learning module on the company's staff dealing policy by a certain date.

Imposing serious enforcement actions for breaches

25 It should be reinforced that breaches of the company's policies for the handling of confidential information and dealings in securities are serious. Where there are violations of the company's policies, the company should discipline employees accordingly depending on the severity of the offence. If warranted, the company should also report the offence to law enforcement authorities.

Example

In Company A, a person who violates the Company's Staff Dealing Policy shall, in addition to any other penal action that may be taken pursuant to law or regulations, also be subject to disciplinary action by the Company. This includes letters of advice, warnings, and termination of employment.

If it is discovered by the Compliance Officer that there has been a violation of the Company's internal compliance policy by a staff member, the Company's Compliance team and human resources unit will be immediately informed. For more serious breaches, the Board and Audit Committee will also be notified. Enforcement action will be instituted following directions from the Company's Board and Audit Committee.

Placing effective technology in place

26 Larger-scale companies may wish to consider using technology to enhance their internal compliance policies. Some examples of measures which can be implemented include sending of firm-wide or project-group specific reminders and warnings, mandatory file encryption procedures, and online e-learning. Please refer to examples in Principle B3.

Principle A3

Conduct regular reviews of the policy and procedures to assure that they are relevant and effective

27 The internal compliance policy should be reviewed regularly, ideally on a yearly basis. This will help to ensure that the internal compliance policy continues to be fit for purpose as the legal and regulatory landscape develops and as the organisation's business grows.

28 Periodic reviews should take into account changes to the organisation's business operations and structure which may impact the scope of securities dealing restrictions specific to the organisation. The internal compliance policy and training should also be updated to reflect changes in technology (e.g. instant messaging and social media), and to take into account any recent cases, guidance and disciplinary action on the handling of confidential information and on dealings in securities.

PART B

Handling And Control Of Information

Principle B1

Restrict the dissemination and sharing of confidential information to reduce any chances of information leakage, which could reduce market integrity

Limit the number of people with access to confidential information

29 Issuers and advisers are encouraged to adopt the "need to know" principle. Under this restriction, confidential information should be disseminated only to people who need the confidential information for the purposes of carrying out their official business duties. The aim of this restriction is to prevent unauthorised access to confidential information, while ensuring that personnel with legitimate reasons are still able to access such information.

Example

Company A discloses confidential information only to those persons who need to know the same in furtherance of a legitimate purpose, the course of performance or discharge of their duty and whose possession of the confidential information will not in any manner give rise to a conflict of interest or likelihood of misuse of the information. Proper policies are in place to ensure that confidential information is only shared with those who need to know the information in order to perform his or her job functions. Managers are required to verify that confidential information is shared only to those who have a legitimate need to know the information.

Persons privy to confidential information adopt among others, the following safeguards in order to preserve the confidentiality of information and prevent its wrongful dissemination:

- Physical documents containing confidential information are kept secure, for example in a locked storage space or locked room
- Computer files have adequate security of login through encryption or passwords
- Shared electronic records and systems have limits on the persons who are granted access

The Compliance Officer and persons in charge of information technology from time-to-time review the safeguards and prescribe other measures to protect the confidentiality of information.

30 It is a matter of judgement for organisations to consider whether the confidential information should be disclosed to a particular person. Information may be disclosed if it is:

- reasonable and needed to enable a person to perform the proper functions of his employment, profession or duties;
- reasonable and is (for example, to a professional adviser) for the purposes of facilitating or seeking or giving advice (for example, about a transaction or takeover bid);
- reasonable and is for the purpose of facilitating any commercial, financial or investment transaction (including prospective underwriters or placees of securities);
- reasonable and is for the purpose of obtaining a commitment or expression of support in relation to an offer which is subject to the Takeover Code; or
- pursuant to court orders or as required by any applicable laws and regulations or the Exchange's listing rules and requirements, or to (or at the direction of) any other regulatory authorities.

The above list of situations is non-exhaustive.

31 If the complexity or urgency of a transaction necessitates more involvement, such access should be a carefully considered decision, with the board and senior management ultimately accountable for the adequate control of the flow of confidential information. The need for dissemination of information to relevant personnel should also be periodically assessed. The flow of information should cease once the person no longer has need of the confidential information.

Exercise caution when communicating confidential matters

32 Persons to whom confidential information is disclosed must ensure that they do not share it with unauthorised persons. In sending emails or messages digitally, the sender must take care in ensuring that the message is sent to the correct party. Inadvertent errors might occur in sending confidential information to unrelated third parties who share similar names and/or phone numbers as the recipient, and the onus in verifying the correct recipient falls on the sender of the message.

Example

Company A's employee code of conduct states that employees shall hold in strictest confidence and shall not use, disclose, remove or transfer whether directly or indirectly, to any person, firm or corporation, any trade secrets, confidential knowledge or data or any proprietary information (including but not limited to information on systems, networks, customer details, business plans, policies and strategies) belonging to/ received by the Company.

Disclosure of such information is only permitted in the following instances:

- Where it is required for the purpose of the performance of duties or functions in the Company
- Where it is lawfully required under the provisions of any written law
- Where it is necessary to detect, prevent or investigate into fraud or risk management
- Where it is authorised by the Board of Directors of the Company

Employees must not breach their confidentiality obligations to third parties in respect of information received in confidence. Any confidential information that is sought from third parties must be done through proper official channels, such as via email correspondence and phone calls, via contact details approved by the third parties or face-to-face meetings with the third party.

As far as possible, employees should adopt a "clean desk"/clear screen policy. Confidential and restricted business information must be secured, and computers and terminals must be logged off or password-protected when not in use.

Implementation of Chinese Walls

33 A Chinese Wall refers to an information barrier created to completely restrict information flow between different departments in the same company. For example, bankers in possession of confidential information relating to a publicly traded company are strictly prohibited from discussing any such information with other employees who do not have any need to know such information.

34 Organisations are encouraged to physically separate certain groups of employees so as to limit the risk of confidential information leaking. Physical barriers such as walls and access controls (e.g. key cards for entry into specific departments) can be erected in the office. Companies can also situate departments which routinely deal with confidential information at a separate site, away from other employees.

35 Aside from physical separation, companies should also look at implementing IT policies which facilitate the control of electronic access to information. Data can be compartmentalised by departments, and companies can assign varying user rights to staff based on their department to easily restrict access to data relevant to the department (e.g. sales personnel will have no access and are unable to access files used by the accounting department).

36 Under certain circumstances, organisations might find it necessary for confidential information to be shared amongst employees of different departments. This process is known as bringing the previously uninformed employee(s) "over the wall". Organisations should actively try to minimise the number of personnel brought "over the wall", and when doing so, the reasons should be documented appropriately. These employees must be restricted from sharing the confidential information until the information has been made public.

37 It is to be noted that while there is what is commonly called a "Chinese Wall" defence to insider trading, the specific conditions set out under Section 226(2) of the SFA have to be met in order for such a defence to succeed. The following requirements must be satisfied:

- the decision to enter into the transaction or agreement was taken by a person other than the officer or partner who was in possession of the information;
- the corporation or partnership had arrangements that could reasonably be expected to ensure that the information was not communicated to the person who made the decision and that no advice with respect to the transaction or agreement was given to that person by a person in possession of the information; and
- the information was not communicated and no such advice was given to the decision-maker.

Example

Company A has adopted a "Chinese Wall" policy which separates departments which routinely have access to confidential information (considered "inside areas") from client servicing departments which deal with sales and marketing or other departments providing support services (considered "public areas"). For specific transactions, further restricted areas may be created within the "inside areas" to limit access only to employees working on that particular deal. The policy states that:

- The employees in the inside areas are not allowed to communicate any confidential information to anyone in the public areas.
- The employees in inside areas may be physically separated from the employees in public areas.
- The demarcation of various departments as inside areas shall be determined by the Compliance Officer/ Compliance department in consultation with the Board.
- Only in exceptional circumstances, employees from the public areas are brought "over the wall" and given confidential information on a need-to-know basis.
- All such instances are documented and kept by the Compliance Officer/ Compliance department.

Maintenance of a privy persons list

38 Practice Note 7.2, Section 6 of the Listing Manual makes reference to keeping a list of persons who have access to confidential information (the "privy persons list"). The privy persons list should typically include information on the identity of the privy persons, the circumstances under which these persons gained access to the information (i.e. became aware or involved in the transaction), and the dates on which these persons first gained access to the information. Advisers should provide the issuers with a list of the people[5] within their firm who have been given access to the issuer's confidential information, and then ensure the list is updated regularly.

39 For the privy persons list[6], it is encouraged that those directly involved in the transaction be listed by name as per their identification card / passport. Prior to the execution of the transaction, issuers might have approached other advisers and/or investors. If confidential information is shared, issuers should keep records of those approached, the dates when meetings were held and the information disseminated to the advisers and/or investors. These details should also be added to the privy persons list.

40 The privy persons list should also state the date on which the person is granted access to the confidential information. A sample of a privy persons list can be found in Appendix A.

41 A chronology of events should be maintained in conjunction with the privy persons list. The list should be started when negotiations/ discussions first commenced until the time the confidential information was announced.

42 Companies are encouraged to implement a system on how and when people are captured on the privy persons list. When placing a person on the privy persons list, the organisation should inform the relevant person of the responsibilities on keeping information confidential. The privy persons list should also be updated if access to information has been removed from the relevant person.

Confidentiality agreements with third parties

43 It is common for issuers to engage advisers to assist them with matters involving confidential information. Issuers will also inevitably share confidential information with transaction parties. As confidential information will be disclosed to external parties, issuers should actively engage their advisers and transaction parties on the controls implemented to prevent leakage of confidential information by them. Issuers are encouraged to sign confidentiality agreements (also known as non-disclosure agreements) with their advisers and potential transaction parties as early as practicable, preferably at the time of engagement of an adviser or prior to exchanging confidential information or commencing substantive discussions with a potential transaction party. If issuers deal with certain advisers and transaction parties on a regular basis, an umbrella confidentiality agreement can be agreed upon between both parties so as to lessen the administrative burden.

44 The confidentiality agreement should set out, at the minimum, the following items:

- An acknowledgement that in the course of the transaction, the parties may have access to confidential information
- An undertaking that each party (i) will not deal in the securities of the company for so long as such confidential information is not generally available to the public; and/or
- (ii) will not deal in the securities of the issuer in contravention of the prohibitions under the SFA, and to procure that its employees do so as well
- The term (lifespan) of the confidentiality agreement

[5] *Alternatively, issuers may enter into arrangements with advisers for the latter to maintain their own privy list which can be provided to authorities.*

[6] *The privy persons list should also include external auditors, lawyers, public relations agencies and other third parties who have access to confidential information.*

- Compliance with the need-to-know principle
- Arrangements to facilitate compliance with the privy persons list requirements
- Confirmation that each party will handle confidential information with the same degree of care that it uses for its own confidential information
- For advisers, to consult the company before speaking to third parties or publicly disclosing that they are acting for the company

Principle B2

Have in place procedures to prevent accidental disclosures

Adopting code names for transactions

45 When engaging in potential price-sensitive transactions, companies should adopt appropriate code names for transactions to conceal the nature of the transaction and the parties involved.

Not to discuss confidential information in public

46 Companies should remind employees not to discuss the details of transactions or to read confidential documents in public places (e.g. airports, planes, lifts and taxis).

47 Issuers will, from time to time, conduct analysts' briefings, hold shareholders' meetings and engage with the media. However, such meetings might create a perception that analysts, institutional investors, fund managers or media have access to information that is not generally available to the public and this may undermine investors' confidence in the existence of a level playing field. As such, it is imperative for issuers to put in place procedures when engaging with third parties. In particular, Practice Note 7.1, section 3.1 of the Listing Manual states that "an issuer should have in place policies to minimise the risk of being perceived to be practising selective disclosure."

48 Such policies might specify that any prepared information intended for briefings and meetings, for example slides or speeches, be pre-released via SGXNET. Alternatively, the issuer can choose to release such information via its own website with an accompanying SGXNET announcement to inform investors that additional information is available on the issuer's website. The second alternative may be preferred if the issuer intends to release large-sized files.

49 Where an issuer inadvertently discloses confidential information during these briefings or meetings, the information disclosed to third parties will no longer be considered confidential for the purposes of the exemption allowed under Rule 703(3) of the Listing Manual. If it has not already done so, the issuer must disseminate the information via SGXNET as promptly as possible. An issuer should, if necessary, request a suspension of trading in its securities or a trading halt.

Example

Company A endeavours not to divulge information to any person (other than within the Company and its advisers) in such a way as to place any person in a privileged dealing position, i.e. selective disclosure is avoided at all times. All disclosures are submitted to Singapore Exchange Securities Trading Limited ("SGX-ST") through SGXNET, and are made available on the Company's corporate website.

In general, confidential information will not be selectively disclosed. However, there may be limited instances where selective disclosure is necessary. One example is the pursuit of the Company's business or corporate objective, such as when the Company is undertaking a major corporate exercise. Another example is due diligence when the issuer is the subject of an acquisition. In these circumstances, selective disclosure may be required to facilitate the exercise. However, such disclosure should be made on a need to know basis and subject to appropriate confidentiality restraints.

However, if any confidential information is inadvertently disclosed, it will be immediately announced to the public via SGXNET and the media.

Proper processes for public announcements

50 Companies should adopt proper processes in releasing public information. A robust disclosure policy in drafting and releasing announcements helps in ensuring that information contained in SGX announcements is accurate while avoiding inconsistencies and errors. The policy should be consistent with applicable rules and regulations, as well as the Listing Manual.

Example

The disclosure policy of Company A is based on the following principles:

- All significant SGX announcements must be circulated to the Board before release.
- The following information should be included in the notice to the Board when a draft SGX announcement is circulated:
  - the proposed date and time of the release of the announcement; and
  - the level of urgency.

All announcements should be circulated to the Board for its reference after release.

Disclosure Committee

To support the Board and to execute the Company's disclosure policy, the Board has established a committee responsible for disclosure issues (the "Disclosure Committee"). The composition of the Disclosure Committee comprises members of the management team such as the CEO, CFO, Financial Controller, Company Secretary, legal counsel, and other relevant management.

The Disclosure Committee oversees and administers the Company's disclosure policy and ensures that the Company complies with its disclosure obligations. The Disclosure Committee also has clear terms of reference which allows some room for flexibility in adapting to the changing business climate. The members of the Disclosure Committee stay abreast of disclosure requirements and periodically review and update the Company's disclosure policy to stay relevant with the latest regulatory, business and legal developments.

Principle B3

Have effective physical document management and information technology controls

51 Issuers and advisers should ensure that physical documents are managed appropriately to minimise leakage of confidential information. It is important that information technology systems and practices are sufficiently secure to ensure that confidential information is not inadvertently disclosed. The levels of security of information may vary depending on the sensitivity of the information and the nature of the company's technology infrastructure. Smaller companies may have less comprehensive or sophisticated infrastructure. Systems and practices that may help include:

- Marking information and documents appropriately
- Having a group email address
- Controlling access to documents containing confidential information
- Encouraging a "clean desk" policy
- Having appropriate password protection on documents and electronic equipment
- Having procedures to handle loss of office property containing confidential information
- Having appropriate measures to manage use of personal devices

Marking information and documents appropriately

52 Issuers and advisers should mark confidential information appropriately. For example, the documents should have a "Confidential" watermark, be kept in folders which are marked "Confidential", and/or emails should have a "Restricted" or "Confidential" marked in the header or before the email message begins. There should be an information classification policy in place.

Having a group email address

53 Issuers and advisers should use a group email address for a project involving multiple parties to reduce potential risks of documents being sent to unintended recipients due to typing errors. The inclusion of particular employees in the group email should be regularly reviewed and updated where necessary.

Controlling access to documents containing confidential information

54 Issuers and advisers should ensure that only authorised personnel are given access to documents and can operate a document management system that has the capacity to record access to files. It is good practice to establish physical segregation of working areas and data files to prevent inadvertent sharing of information during discussions or unattended work files.

Example

Company A does not allow any visitors into the Company's working area unless accompanied by an authorised staff. It is the responsibility of that authorised staff to escort his visitors at all times whilst they are in the Company's premises and to see them off the premises when they leave. Company A's Staff Handbook also reminds staff to be alert to apparent strangers taking packages into or out of the Company's premises.

Company A's different departments are located in various locations throughout the office which are separated by doors where access is controlled by access systems.

The data files stored by a business unit on the server cannot be accessed by employees in other units or by third parties.

Example

Sample of Staff Handbook on handling of confidential information

You must (i) not use any Confidential Information for your benefit or for the benefit of any person other than the Company, and (ii) restrict access to Confidential Information only to those on a need to know basis for business purposes. Additionally, remove documents, files or laptops containing such Confidential Information from the office only when absolutely necessary, and minimise entry by employees and third parties who are not authorised to access such Confidential Information into areas of the office where such Confidential Information is easily accessible or can be viewed. On these occasions, you should ensure that precautions are taken to protect the confidentiality of the information.

During the course of your employment, you may be given and will generate emails, documents, reports, contracts and other documents and data concerning the Company. All such records and data, whether maintained in hard copy or soft copy, belong to the Company. Any communication of such records and data or communication relating to official business must go through the Company's authorized communication platforms such as the Company's official email system, and must not be communicated through private or personal platforms. Prior to leaving the Company, you will be required to return all such documents to the Company and are not allowed to retain any copy of these documents or make any notes regarding such documents. You must not disclose or use any Confidential Information after leaving the Company.

You must keep Confidential Information in strict confidence at all times.

Encouraging a "Clean desk" policy

55 Issuers and advisers should ensure that physical copies of documents containing confidential information are securely stored when not in use and disposed of when no longer required, with access restricted to authorised staff only. It is good practice to have policies restricting the downloading of office-related emails or documents to employees' personal devices.

Example

Company A's Clean Desk Policy provides that:

- Employees are expected to ensure that all confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied and shut completely down at the end of the work day.
- Any confidential information must be removed from the desk, stored away or locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing confidential information must be kept closed and locked when not in use or when not attended.
- Keys used for access to confidential information must not be left at an unattended desk.
- Laptops and tablets must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing confidential information should be immediately removed from the printer.
- Upon disposal confidential documents should be shredded in official shredder bins or placed in lock confidential disposal bins.
- Whiteboards containing confidential information should be erased.

Having appropriate password protection on documents and electronic equipment

56 Issuers and advisers should implement appropriate password protection and/or encryption for documents commensurate with their sensitivity and confidentiality. In addition, appropriate security measures should be in place on electronic equipment (such as laptops and mobile phones) which are used to access and/or store confidential information.

Example

Company A allocates dedicated printers, faxes, photocopiers, data rooms and other mechanisms for certain market-sensitive transactions.

Company A installs password-protection mechanisms for all soft copy documents (or access to such documents, e.g. laptops, smartphones, tablets, USB drives and other storage media containing confidential information). Automatic locking will be activated after periods of inactivity on these devices.

Having procedures to handle loss of office property containing confidential information

57 Issuers and advisers should require all staff to take care of and safeguard office property containing confidential information in their possession (whether inside or outside the office). There should be procedures in place in the event of loss of such office property. Issuers and advisers should designate internal functions to whom loss/theft is reported, and install software allowing for remote deletions of information when electronic equipment (e.g. a tablet or smartphone) is misplaced.

Example

Company A's Staff Handbook provides examples of property that may contain or provide access to confidential information, including but not limited to the following:

- laptops, tablets, Blackberry devices, mobile phones and other similar equipment or devices issued by the Company, including any information that has been stored electronically on such devices;
- office keys, access cards and/or other office security passes issued by the Company; and
- information that has been stored electronically on devices owned by the staff (for example, emails, attachments and soft copies of documents, financial models or presentations that are downloaded to the staff's personal laptop, tablet, mobile phone, personal computer or similar equipment or device).

Staff must ensure that laptops, tablets, Blackberry devices, mobile phones and other similar equipment or devices are password protected and should not reveal their password to any other person.

Any loss or theft of office equipment or devices must be reported to management and the information security team immediately. A police report must be made within 48 hours of the loss and a copy of the police report is to be given to management.

Having appropriate measures to manage use of personal devices

58 If the issuer permits the use of employee personal devices such as personal mobile phones and personal computers for corporate communications, the issuer should implement appropriate measures to manage related risks (such as those relating to security, confidentiality, record retention and data protection). These measures could include a detailed bring-your-own-device policy requiring employees to comply with device management and IT security policies.

Example

Company A's Staff Handbook provides that staff may download office-related emails or documents to their personal mobile phones, tablets and personal computers or similar electronic devices in the course of their work. If so, staff are reminded to:

- keep such downloaded information confidential; and
- delete such downloaded office-related emails or documents from their personal devices on a regular basis, or when such information is no longer required to be retained.

PART C

Restrictions Against Dealings In Securities

Principle C1

Institute a "black-out period" and/or "trading windows", to limit the time frame that dealing in the company's securities is permitted; maintain a policy that staff should not deal in the company's securities based on speculation or short-term considerations

Instituting a "black-out period" and/or "trading windows"

59 A "black-out period" refers to a period of time during which dealing in the issuer's securities is prohibited. During such time, any requests for dealing in the issuer's securities will be blocked or rejected.

60 The "black-out period" should be at least two weeks before the announcement of the issuer's financial statements for each of the first three quarters of its financial year and one month before the announcement of the issuer's full year financial statements (if the issuer is required to announce quarterly financial statements), or one month before the announcement of the issuer's half year and full year financial statements (if the issuer is not required to announce quarterly financial statements).

Example

Company A reports its results quarterly and adopts a "black-out period" policy. The "black-out period" in respect of declaration of financial results is applied to all staff and management. Dealing in the company's securities is prohibited for (i) the two weeks preceding the announcement of the company's quarterly results; and (ii) the one month preceding the announcement of the company's full year financial results.

In addition, Company A may from time to time impose "black-out" periods for specific persons or classes of persons who are reasonably expected to be in possession of inside information, for purposes including: (i) the declaration of financial results or dividends; (ii) changes in capital structure of the company; (iii) potential acquisitions, investment plans, mergers, disposals and such other transactions; (iv) litigation action; and (v) changes in senior management and key personnel.

61 A less common approach is the implementation of "trading windows" for senior management and employees working within certain departments (such as finance, sales and business development, investor relations and legal), employees who report directly to the Chief Financial Officer ("CFO Direct Report") and employees who report directly to a CFO Direct Report, and any administrative assistant to any of the aforesaid persons (collectively, the "Key Insiders"), who are persons identified as being more likely to possess inside information in the course of their work. Trading windows refer to fixed windows of time within which Key Insiders may deal in the company's securities, and typically range from 30 to 60 days following the announcement of the company's financial results, and are not applicable to other staff. The length of the trading window depends on several factors, including, amongst others, the sensitivity of the information handled and the frequency of confidential information being generated. Dealing in the company's securities outside specified "trading windows" is generally prohibited.

62 For "trading windows", it is important to remind Key Insiders in the staff dealing policy that insider dealing is strictly prohibited at all times. Just because dealing in the company's securities is allowed during the trading window does not mean that trading is permitted if the Key Insider is in possession of confidential information at the time of the transaction. Likewise, if a "black-out period" is instituted, it is important to remind staff that in the period preceding and following the black-out period, restrictions against dealings in securities and the requisite pre-clearance and/or notification procedures continue to apply.

Example

Company A adopts a "trading window" policy for its Key Insiders. The policy states that dealing in the Company's securities is generally prohibited, except for specified periods where the "trading window" is opened. Company A opens a "trading window" for the thirty-day period starting from the trading day after the announcement of its financial results, or after the Company's annual general meeting.

Before each "trading window" is opened, Company A sends out email notifications to remind all Key Insiders that insider trading is prohibited at all times, even when the "trading window" is open. The reminder states that if in doubt, clarification should be sought from unit heads or the Compliance team before dealing in the Company's securities.

Additionally, staff are reminded that they must notify the Company through Company A's electronic portal, or by email to certain designated officers, within 48 hours of dealing in the Company's securities in any account(s) maintained or controlled by them and/or their associates. Such notification must be in a prescribed form and state the full name of the beneficial owner(s) of the securities, their relationship to the staff member, the date and approximate time of dealing, and the number and price of securities dealt. No other forms of notification e.g. verbal or SMS notification are allowed.

Specifying policies in relation to short-term dealings

63 In general, organisations should discourage their staff from engaging in speculative transactions involving the company's securities, as such actions may be considered improper and inappropriate. Additionally, staff should be advised not to deal in the company's securities on short term considerations, as short term trading can be a key indicator of insider trading, particularly when done regularly or in large amounts.

Example

Company A's Staff Dealing Policy states that all staff and management should avoid engaging in any of the following activities with respect to the Company's securities:

- Trading on a short term basis – short term investment holding periods (less than three months) are discouraged
- Short Selling – as it would display an expectation that the Company's securities will decline in value, suggesting that the seller has no confidence in the Company or its short term prospects
- Speculative trading – including buying and selling "put" and "call" options and hedging transactions, as dealing in the Company's securities should be for investment purposes rather than being based on speculative considerations
- Purchasing the Company's securities on margin – so as to avoid margin sales or foreclosure sales which may occur when the individual is in possession of inside information

Principle C2

Establish proper pre-dealing and post-dealing procedures, and ensure proper audit trails

Pre-dealing procedures

64 It is good practice for all staff and management of listed issuers to be subject to pre-dealing approvals and/or notifications for trades in the issuer's securities. At the minimum, pre-dealing approvals and/or notifications should be imposed on all senior management and all persons who may come into possession of inside information. In addition, for financial institutions and corporate service providers which are likely to manage or undertake investments in multiple listed securities, pre-dealing approvals should be sought for trades in all listed securities.

65 The requisite internal approval level for dealing requests should be determined with regard to the overall organisational structure and other delegations of the applicant (if any). Organisations may wish to provide for tiered approval requirements depending on (i) the unit function and designation of staff, and/or (ii) a materiality threshold such as the number of shares/ units proposed to be traded.

66 The pre-approval and/or notification process should be imposed on a continuous ongoing basis, including during trading windows (if any). Depending on the needs and capabilities of the organisation, approval requests can take the format of an online form through an electronic portal, through email by adopting a prescribed format with necessary details, or through written and signed requests.

Example

On Company A's staff dealing approval system, the following details need to be submitted when a new request is put in for dealing in the Company's securities:

Applicant Details

- Staff name
- Staff unit and designation

Trade Details

- Type of transaction (Buy, Sell, Others (specify))
- Type of security
- Name of security
- Number of shares or units
- Approver (Unit head/ Compliance Officer/ CEO/ Chairman, as applicable)
- Remarks
- Attachments, if any
- Proposed trading dates

Additionally, applicants will need to tick a check box at the bottom of the request form, to indicate their acceptance of a declaration that he/ she is:

- fully aware of the prohibitions, penalties and liabilities on insider dealing;
- fully aware of the prohibitions, penalties and liabilities on false trading, market rigging transactions and securities market manipulation; and
- fully aware of the requirements set out in the Company's Staff Dealing Policy.

The declaration also states that the applicant is not in possession of inside information, and warrants that the proposed dealing is not in contravention of the prohibited dealing provisions of the SFA and Staff Dealing Policy, and that by dealing he/ she will not contravene any of the prohibited dealings provisions of the SFA and the Staff Dealing Policy.

67 Once approval is granted, the applicant should be notified of the number of shares or units that he/ she may trade in, the validity period of the approval, and a notification that the approval will automatically be deemed to be withdrawn if the applicant becomes aware of inside information prior to trading.

Example

Company A's Staff Dealing Policy extends to all staff and senior management. In respect of staff dealing approvals, each person covered under the Policy will need to obtain prior approval before making a trade in securities specified under the Policy.

Staff will have their dealing requests approved by their respective department heads and, in the case of the CEO and the CFO, their requests will be approved by the Chairman of the Audit Committee.

Post-dealing procedures

68 Proper post-dealing procedures should also be implemented. It is good practice for organisations to keep a record of the actual securities traded, or if no transaction was executed.

Example

Company A uses an electronic system to record its staff dealing requests, approvals and completed transactions. An approval to deal in the Company's securities lasts for three days, starting from the date that the approval was granted. After the validity of the dealing approval has elapsed, the electronic system sends an automatic reminder to the applicant to update the details of any transaction in the Company's securities that had been executed.

The applicant will be required to fill in and submit a declaration form stating the beneficial owner(s) of the securities, their relationship to the applicant, the date and approximate time of dealing, and the quantity and price at which the Company's securities were traded. A "nil" response is also required, if the applicant did not proceed to make any trade after receiving a pre-dealing approval.

Company B does not have in place an electronic system to record the completion of pre-cleared dealings in the Company's securities. Instead, at the time of filing a request to deal in the Company's securities, applicants are required to provide an undertaking that they will file the details of any transacted pre-cleared deal within two trading days of execution. The details of the transaction must be recorded using a prescribed form, and must be submitted to the Company's Compliance Officer. A transaction which is not undertaken will also need to be reported as such.

69 Some transactions may be excluded from the need for pre-dealing approvals, including situations where trading is passive, or outside the individual's control. In such cases (and provided that the transaction was not made when the individual was in possession of any inside information regarding the company's securities), pre-clearance for dealing in the company's securities may not be required. Examples of such situations include:

- participating as lenders in securities borrowing and lending programmes;
- acceptance of shares or exercise of options under the company's employee share plans;
- acceptance of scrip dividends, bonus issues or takeover offers;
- dealing under an offer or invitation made to all or most of the security holders, such as subscription for entitled rights or equal-access share buyback; and
- transfers of the company's securities between an individual and their spouse or other family member.

Notwithstanding that such trades may not be subject to pre-dealing approvals, organisations can consider obtaining post-trade declarations for the execution of such trades, as a matter of good practice and for prudent record-keeping.

Ensuring proper audit trails

70 Organisations should carry out regular monitoring to ensure that their internal compliance policy on dealings in securities is robust and working well. In particular for financial institutions, this may include periodic reviews of trading accounts belonging to staff, to ensure compliance with post-dealing processes. It also entails keeping records of all trading accounts belonging to staff, including contracts for difference or nominee accounts.

Example

Company B, which is a financial institution, carries out regular monitoring on compliance with its policies on dealings in securities. Its internal audit team carries out random audits on particular employees, transactions and business units, to ensure that the Company's internal compliance policy is being followed. In particular, internal audit will check that staff dealing approvals have been obtained before an employee transacts in the company's securities. This is done by taking a random sampling of staff and senior management. The identified persons' securities transaction statements will be checked against staff dealing requests and approvals made in the same time period for consistency.

For transactions, internal audit will check that confidentiality agreements have been signed with all advisers and counterparties to safeguard the flow of confidential information. They will also check that Chinese Walls and codenames have been put in place, and that adequate encryption or limited access has been used to protect confidential documents. Project registers and completed transactions for the year should be checked against the projects and companies submitted to Compliance for the purposes of updating the "restricted list" and "watch list".

Share Buybacks

71 Undertaking share buyback exercises during periods when the issuer is in possession of inside information may be construed as insider trading, particularly if the persons authorised to give instructions for the account used to make the trade are privy to such inside information. To avoid such situations, issuers should also ensure that they are not in possession of inside information when implementing a share buyback. It should be noted that a company is also a legal person and thus is subjected to the relevant rules against insider trading.

Example

Company A sought approval from shareholders for a share buyback mandate during its annual general meeting. The circular states that because the listed company would be regarded as an "insider" in relation to any proposed purchase or acquisition of its issued shares, the Company will not undertake any purchase or acquisition of shares pursuant to the proposed mandate at any time after a price-sensitive development has occurred until the inside information has been publicly announced.

In particular, the Company will not purchase or acquire any shares pursuant to the proposed mandate during the period commencing two weeks before the announcement of the Company's financial statements for each of the first three quarters of its financial year and one month before the announcement of the Company's full year financial statements.

Principle C3

Maintain a "restricted list" and "watch list" of securities

72 Financial institutions and companies which manage or undertake investments in multiple listed securities such as professional service providers should confidentially maintain a "restricted list" of securities for which trading is strictly prohibited for either all staff or only staff who are privy to, or likely to have access to, inside information about other companies". The "restricted list" should be maintained by the Compliance team and should not be shared with other staff. The aim of having a "restricted list" is to prevent dealing in other companies' securities when required by laws or regulations, or where the organisation's staff and/or management are or may be in possession of inside information about such other companies.

73 These organisations can also consider maintaining a "watch list", which keeps a record of all listed companies whose inside information could potentially be made known to the organisation and/or its employees in the course of their work/ dealings. The "watch list" will be more relevant to issuers involved in multiple investments in listed securities, such as financial institutions and professional service providers. Having a "watch list" is helpful as a surveillance tool to monitor and spot irregular trades conducted by employees where the potential for insider trading exists.

Example

Company A employs the use of both a “restricted list” and “watch list”. Both lists are maintained by the Compliance team and are kept highly confidential.

The “restricted list” is used to limit employees from trading in specific securities, when a market-sensitive transaction is soon to go public, or when trading by the entire Company A and its personnel is restricted under laws and regulations. Restrictions from dealing in securities on the “restricted list” would apply to designated persons which may have access to information regarding market-sensitive transactions. The restriction may also be extended to all staff and management where necessary. For example, when Company A is entering into negotiations for the potential acquisition of Company C, Company C’s securities would be placed on the “restricted list” and all staff and management would be prohibited from dealing in Company C’s securities. Dealings in securities on the “restricted list” are be blocked or disallowed at the time of pre-clearance.

The “watch list” is used by the Compliance team to monitor trades made by employees that suggests that inside information may have been used improperly. When Company A has or is likely to have inside information as a result of its client, supplier, distributor, investment banking, advisory or other relationships, all affected companies will be added to the “watch list”. Examples include companies which Company A has entered into discussions for a joint venture with, suppliers who have just informed Company A that they are in slight financial difficulty, and companies who have signed an agreement with Company A to enter into a consortium to bid for an upcoming project. The responsibility to inform Compliance of all on-going and potential projects and the companies involved lies with the unit head of each department. The companies may be removed from the “watch list” when Company A is no longer in possession of any inside information relating to such companies, for example when a public announcement has been made regarding the proposed transaction.

The “restricted list” is used to limit employees from trading in specific securities, when a market-sensitive transaction is soon to go public, or when trading by the entire Company A and its personnel is restricted under laws and regulations. Restrictions from dealing in securities on the “restricted list” would apply to designated persons which may have access to information regarding market-sensitive transactions. The restriction may also be extended to all staff and management where necessary. For example, when Company A is entering into negotiations for the potential acquisition of Company C, Company C’s securities would be placed on the “restricted list” and all staff and management would be prohibited from dealing in Company C’s securities. Dealings in securities on the “restricted list” are be blocked or disallowed at the time of pre-clearance.

The “watch list” is used by the Compliance team to monitor trades made by employees that suggests that inside information may have been used improperly. When Company A has or is likely to have inside information as a result of its client, supplier, distributor, investment banking, advisory or other relationships, all affected companies will be added to the “watch list”. Examples include companies which Company A has entered into discussions for a joint venture with, suppliers who have just informed Company A that they are in slight financial difficulty, and companies who have signed an agreement with Company A to enter into a consortium to bid for an upcoming project. The responsibility to inform Compliance of all on-going and potential projects and the companies involved lies with the unit head of each department. The companies may be removed from the “watch list” when Company A is no longer in possession of any inside information relating to such companies, for example when a public announcement has been made regarding the proposed transaction.

74 Advisers to listed issuers should also maintain “restricted lists” and “watch lists”. The securities on these lists should include securities of clients, as well as the securities of any listed companies linked to specific transactions which the advisers are working on. The “restricted list” is mandatory for firms involved in corporate finance activities and is in line with Chapter 16 of the SGX-ST Rules.

Appendix A

Sample Privy Persons List

Name of Listed Company :

Date of Announcement of Confidential Information :

Full Name as per NRIC / Passport	NRIC / Passport No.	Business Contact Nos.	Mobile Contact Nos.	Company	Designation	Circumstances under which person became aware or involved in said transaction	Date of 1st awareness or involvement

Singapore Exchange

Beijing ▪ Chicago ▪ Hong Kong ▪ London ▪ Mumbai ▪ Shanghai ▪ Tokyo

2 Shenton Way
#02-02 SGX Centre 1
Singapore 068804

main: +65 6236 8888
sgx.com