17 The Protection Obligation

17.1 Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. This obligation of organisations to protect personal data is referred to in these Guidelines as the Protection Obligation.

17.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

17.3 In practice, an organisation should:

a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;

b) identify reliable and well-trained personnel responsible for ensuring information security;

c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and

d) be prepared and able to respond to information security breaches promptly and effectively.

17.4 In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors may be considered:

a) the size of the organisation and the amount and type of personal data it holds;

b) who within the organisation has access to the personal data; and

c) whether the personal data is or will be held or used by a third party on

behalf of the organisation.

Examples of security arrangements

17.5 Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. The following tables list examples of such measures.

Examples of administrative measures an organisation may use to protect personal data:

- Requiring employees to be bound by confidentiality obligations in their employment agreements;
- Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;
- Conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data; and
- Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

Examples of physical measures an organisation may use to protect personal data:

- Marking confidential documents clearly and prominently;
- Storing confidential documents in locked file cabinet systems;
- Restricting employee access to confidential documents on a need-to-know basis;
- Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops;
- Proper disposal of confidential documents that are no longer needed, through shredding or similar means;
- Implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security (e.g. registered post instead of normal post where appropriate);

- Providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and
- Confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data.

Examples of technical measures an organisation may use to protect personal data:

- Ensuring computer networks are secure;
- Adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate);
- Encrypting personal data to prevent unauthorised access;
- Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period;
- Installing appropriate computer security software and using suitable computer security settings;
- Disposing of personal data in IT devices that are to be recycled, sold or disposed;
- Using the right level of email security settings when sending and/or receiving highly confidential emails;
- Updating computer security and IT equipment regularly; and
- Ensuring that IT service providers are able to provide the requisite standard of IT security.