

Annex – Elaboration of selected controls for preventing and detecting the loss or leakage of customer data

A. Data classification and risk assessment

As all data processed by AIs for their clients could be considered as customer data, AIs should classify the data into different levels of sensitivity or risks so as to determine the protection required, in line with section 3.1 information classification and protection of the SPM module on “General Principles for Technology Risk Management”. In this connection, AIs should conduct proper risk assessment to design and implement layers of security controls (covering both IT and non-IT controls) to protect customer data, commensurate with the level of risks assessed.

B. Data security policies and awareness

AIs should develop formal policies and procedures on data security to safeguard customer data, covering areas on, among others, system controls, physical security controls, mobile computing, and outside service providers. The policies and procedures should be in line with the relevant supervisory guidance issued by the HKMA from time to time. Where personal data are involved, the policies and procedures, including those to be followed by the relevant service providers, should also be in line with PDPO and any relevant codes of practice, rules or guidance¹ issued or approved by the Privacy Commissioner.

Moreover, AIs should formulate an effective awareness programme reminding staff at least annually of the importance of complying with the data security policies and procedures, prompt reporting of potential leakage or loss of customer data and the possible disciplinary actions for any violations.

C. Logical access controls of customer data

AIs should identify the locations of customer data residing in different parts of AIs’ networks and systems and ensure that adequate logical access controls are in place at different levels (e.g. application level, database level, operating system level, network level) to prevent unauthorized access to customer data and unauthorized/erroneous transmission of customer data to external parties. These controls should include: (i) the rights to access customer data and transmit customer data to external parties should be granted on a need-to-have basis only; (ii) the tools for massive download of customer data can be used only upon proper approval from the management and the use should be promptly revoked if the approval is no longer valid; (iii) proper re-certification² of user access and access rights should be performed at least annually (more frequently for systems or user access rights of higher risk or sensitivity); (iv) audit trail should be enabled whenever there is a need for detection of unusual activities

¹ For instance, the Privacy Commissioner has issued guidance note on “Guidance on the Proper Handling of Customers’ Personal Data for the Banking Industry”, “Guidance for Data Users on the Collection and Use of Personal Data through the Internet”, and “Guidance on Personal Data Erasure and Anonymisation” as well as the information leaflet of “Outsourcing the Processing of Personal Data to Data Processors” and “Online Behavioural Tracking”.

² In general, re-certification entails a review of the entitlement of staff members’ access to systems or storage for customer data with proper attestation.

(e.g. potentially unauthorized access to customer data, suspicious massive download of customer data); (v) regular reviews of audit trails should be conducted, supported by effective follow-up actions; (vi) system and network infrastructure with robust security controls, including those stipulated in the SPM module on “General Principles for Technology Risk Management” (such as section 3.4 on system security and section 6 on communications network) should be in place to guard against unauthorized access to customer data by internal or external parties; and (vii) remote access by AIs’ staff or service providers from external networks (including from the Internet) to the customer data stored in the AIs’ or service providers’ systems should be subject to robust authentication (e.g. two-factor authentication) and the data being transmitted should be subject to strong data encryption.

D. Controls over transmission of consumer data³

Given the importance of ensuring that consumer data are adequately protected, AIs should implement effective system controls to prohibit unauthorized transmission of consumer data from their internal systems to outside networks/systems via Internet services that could store data (e.g. web-based e-mail, social media sites or websites providing file storage function) or high-risk software (e.g. peer-to-peer file sharing software). For instance, the desktop computers of AIs’ staff members who have access to consumer data but do not have an operational need to transmit consumer data to outside networks/systems should normally be restricted from having access to those Internet services or high-risk software in order to avoid potential leakage of customer data.

As regards staff members who are allowed to transmit data to outside networks/systems through legitimate channels such as corporate e-mails, AIs should put in place effective system controls for prompt detection of unusual or potentially suspicious activities regarding access or transmission of consumer data. For instance, AIs should have the ability to identify cases where consumer data are leaked via corporate emails to outsiders by staff members who do not have an operational need to send out those data. Even for staff members who are authorized to send out consumer data to outside networks/systems, AIs should be capable of detecting quickly activities such as outbound transmission of abnormally large quantity of consumer data (including those compressed files). Using a risk-based approach, proper and timely follow-up actions should be taken upon the detection to ascertain whether leakage of consumer data has actually happened.

To serve as an effective deterrent to unauthorized transmission of consumer data to outside networks/systems, AIs should consider highlighting to their staff members the existence of their detection controls (without disclosing the details of the detection rules) and the disciplinary actions that may be taken in relation to unauthorized transmission of consumer data.

³ For the purpose of this circular, consumer data include (i) sensitive information about the accounts or transactions of personal banking customers (e.g. private banking or retail banking customers), and/or (ii) personal information such as names, personal phone numbers, residential addresses and HKID / passport information of personal banking customers. For instance, data about account numbers together with the associated account balances / transaction details are generally regarded as sensitive information about the accounts or transactions. Another example is information about the account numbers of private or retail banking customers together with the names of the account holders.

Although the controls in this section only cover consumer data, AIs should consider implementing such controls, where appropriate, to protect customer data other than consumer data.

E. Controls over storage of customer data

AIs should take effective measures to address the risk of unauthorized downloading of customer data to portable storage media (e.g. USB drives) and loss of such media containing customer data. In this connection, AIs should disable the portable storage media ports of those computers of staff members who do not have an operational need to download data to such media. For staff members who have an operational need to download data from their computers to such media, AIs should implement system controls such that only their registered media could be used for the download and the following security measures should be in place:

- (i) effective system controls (e.g. through USB control software or USB drives with an embedded encryption feature) for enforcing password with strong data encryption to protect the data stored on these media;
- (ii) procedures advising staff members to erase customer data from such media in a timely manner after use; and
- (iii) maintaining proper records (e.g. a register of the portable storage media together with the relevant approval records of usage) on the usage of such media and immediate reporting of any loss of the media to, and follow-up actions by, designated officers or designated management committees, which are chaired by senior management, of AIs.

In addition, AIs should implement effective controls for prompt detection of unusual downloading activities that may involve customer data. For instance, AIs could enable logging of data downloading to those media and perform periodic sample checks on whether customer data have been downloaded without authorization. Another example is that AIs could implement system controls to detect suspicious downloading activities (e.g. downloading of customer data by staff members who are not supposed to have access to, or download, such data; downloading of large files which may include abnormally large quantity of consumer data). Again, proper and timely follow-up actions should be taken to confirm whether those activities amount to unauthorized leakage of consumer data.

If AIs' computer backup tapes containing customer data need to be regularly transported outside of their premises, AIs should also implement similar controls as mentioned (including, among others, strong data encryption, erase of data after the tapes' retention cycle, proper records and immediate reporting of loss) on the computer backup tapes. For one-off or ad-hoc transportation of tapes containing customer data, AIs should also implement similar controls or alternatively deploy robust physical security controls (refer to section G) over the tapes during the process.

For all media (including paper and electronic media) where customer data is stored, AIs should establish secure processes for disposal and destruction of customer data stored in such media, in line with section 3.1 information classification and protection of the SPM module on "General Principles for Technology Risk Management".

F. Controls over personally-owned computing devices

In principle, AIs should require staff members to use only the computing devices provided by AIs for storing or accessing AIs' customer data. Alternatively, AIs should fully comply with the standard of stringent minimum controls developed by the Hong Kong Association of Banks (HKAB) on Bring-Your-Own-Device (BYOD) if they allow the use of BYOD for work. For the avoidance of doubt, we expect AIs to be prepared to implement additional stringent controls related to BYOD in accordance with their data classification and risk assessment results whenever there is a need to protect their systems and networks.

While HKAB's standard is developed for BYOD, the security controls applicable to AIs' own computing devices for accessing or storing customer data should be as stringent as HKAB's standard, where applicable, as well as any other relevant controls stipulated in the SPM module on "General Principles for Technology Risk Management" (such as section 3.5 on controls specifically related to mobile computing).

G. Physical security controls over and office environment related to customer data

AIs should identify the locations within and outside their premises (including service providers) where their customer data are stored or can be accessed. They should satisfy themselves that adequate physical security (including physical access controls, security guards and surveillance cameras) is in place in those locations in order to safeguard customer data against theft or unauthorized access. When AIs or their service providers (e.g. couriers) need to relocate or transport their systems, facilities, records or other assets that contain customer data, they should arrange adequate physical security controls to protect those assets and data during the relocation or transportation. Adequate reconciliation or inventory check should be performed as soon as practicable during and after the relocation or transportation to ensure that no customer data are lost in transit.

AIs should implement controls over their premises or service providers that process or have access to large quantity of sensitive customer data (e.g. call centres, customer document imaging or processing centres, etc.) to reduce the risk of customer data theft (e.g. staff taking away copies of customer data without permission). If appropriate, such controls may include, among others: (i) enforcing a paper-free working environment and disallowing printing and copying of customer data (e.g. screen capturing of customer data); (ii) adequate controls or monitoring over staff members' use of high-risk items (e.g. bags, cameras, mobile phones with a camera function) in the working desks that may assist data theft; (iii) enforcing an open desk working environment for the ease of monitoring or detecting data theft (e.g. photo shooting of customer data).

H. Periodic audits over customer data protection

AIs should conduct periodic audits on the adequacy and compliance status of their controls on customer data protection. Such audits should be conducted by an independent party (such as the AI's internal audit function) with the necessary expertise, and any significant issues should be brought up to the senior management and/or Audit Committee for attention and necessary actions.

I. Other controls over service providers

For outsourcing arrangements that involve storage of and/or access to AIs' customer data, AIs should require their outsourcing operators and other service providers that store, transport or have access to customer data to comply with the AIs' data security policies and procedures including the controls set out in this document. AIs should implement effective controls to monitor and validate the service providers' compliance situation. Such requirements should be specified clearly in the agreements and AIs should conduct a regular assessment (e.g. on an annual basis) to ensure that the service providers comply with all relevant requirements.

In addition to the controls set out above, where there is an operational need (e.g. for customer statement printing) for AIs to transmit customer data to their service providers over public network, strong data encryption should be in place to protect the customer data during transmission.