Data Loss Protection Guidelines

For Insurance Agents

By *Insurance Standing Committee for Cyber Security (ISCCS)*

9 October 2023

Change History

Version	Change Description	by	Date
1.0	Initial Official release	ISCCS	6 Feb 2017
1.1	Amendments of Guidelines from best practice to basic requirements	ISCCS	20 Jun 2018
2.0	Alignment of Guidelines to MAS Notice on Cyber Hygiene	ISCCS	1 Sep 2019
3.0	Added more Guidelines under Chapter 3. To be effective from 1 Jan 2024	ISCCS	9 Oct 2023

CONTENTS

1. Introduction

Insurance agents[1] handle sensitive information such as customer[2] personal information, medical and insurer records. It is thus important for insurance agents to understand the risks of managing and handling such sensitive information and take steps to manage these risks.

The Life Insurance Association ("LIA") and General Insurance Association ("GIA") have established the Data Loss Protection Guidelines for Insurance Agents ("the Guidelines"). The objective of the Guidelines is to provide insurance agents with the basic requirements for managing and handling sensitive information and promote the adoption of these requirements.

Agents are expected to adopt the Guidelines in order to comply with MAS Notice on Cyber Hygiene. This guideline will take effect 1 Jan 2020.

2. Applicability of the Guidelines

- The Guidelines are standards of industry best practices for insurance agents. All agents are expected to abide by the guidelines.
- The Guidelines apply to all devices (that is not issued by their respective insurers[1]) used by insurance agents in the sales and servicing of insurance products or for the collection of customer information.
- If an insurance agent is governed by other Data Loss Protection ("DLP") requirements, the insurance agent is advised to comply with the stricter DLP requirements.
- The Guidelines do not recommend specific security solutions or vendors. For such information, insurance agents are advised to approach their respective insurers.
- This guideline applies to all endpoint devices (e.g. laptops, desktops, tablets, mobile phones) that the agents used to process and store clients' data. For network/ infrastructure devices and/ or servers, agents should seek professional assistance (be it from their respective insurer or third party consultant) to ensure that they comply with the MAS Notice on Cyber Hygiene.

[1] For devices issued by the insurers, the insurers will be responsible to ensure security on those devices

3. Guidelines on Good Cyber Hygiene Practices

The MAS Notice on Cyber Hygiene requires the adoption of 6 basic cyber hygiene practices.

3.1 Administrative Accounts

- It is expected that agents are the administrator of their own personal devices.
- Agents are recommended not to share devices that are used for their agents business and/or house clients.
- If sharing of the devices cannot be avoided, e.g. the devices are family devices, then the agents should set up separate accounts for each individual using the device. Administrative accounts should not be given to another person.
- Agents are also expected to adopt password best practices including:
    - Passwords should not be shared.
    - Passwords should be made up of alphanumeric characters. (*e.g. S0tj!690a*)
    - Passwords should be at least eight characters long.
    - Passwords should be changed periodically (*e.g. it is recommended that password should be changed at least once every 6 months*), unless compensating controls (e.g., 2FA) are implemented.
    - Previously used passwords should not be reused for a period of time. (*e.g. it is recommended that password should not be reused for at least 10 password change cycle*)
- Agents should set screen lock settings to auto-lock after not more than 15 minutes of inactivity. Agents should also screen lock before moving away from the power-on device.

Additional Notes for Mobile Devices

- Mobile devices should not be shared.
- Device password or biometric authentication (e.g. facial recognition) should always be enabled on mobile devices.

3.2 Security Patches

- Agents are expected to regularly check for security patches that are available for the Operating System "OS" of their devices as well as any software that are installed on the devices. (*e.g. For laptops and desktops running Windows, insurance agents can turn on "Automatic update" in the control panel. For MacBook or iOS, agents can download updates from the AppStore periodically.*)
- Security patches should only be downloaded and installed from trusted and official sources.

- Any security patches should be implemented at the earliest possible time.
- Agents should not use OS and software that have reached end of life (i.e. no longer supported by their manufacturer[2]).

3.3 Security Standards

- Laptop or desktop hard disk containing customer data should be encrypted[4] (*e.g. Agents can use Windows Bitlocker[9] to encrypt laptop or desktop hard disk. Alternatively, agents can use third party encryption software recommended by insurers to encrypt the hard disk*.)
- Customer data or payment information should be encrypted before being transferred to any storage media including portable storage devices and cloud-based storage[5]. (*e.g. Agents can either encrypt the storage media, or encrypt each record/file.)*
- Customer data or payment information should be securely erased using data destruction software[6] before disposal of the devices. *(E.g. Agents can use data destruction software recommended by insurers to erase the data stored on the hard disk or storage media.)*

Additional Notes for Mobile Devices

- Software with remote wipe capability should be installed and enabled on the mobile devices *(e.g. iPhone users can enable the "find my phone" feature on iOS; Android users can turn on "Android Device Manager" under device setting)*.
- The encryption features should be enabled in the security settings of the mobile devices if available.
- Mobile devices should not be jail-broken[7] or rooted[8].

3.4 Anti-Virus and Malware Protection

- Anti-virus software should be installed.
- Anti-virus software and virus definition files[3] should be kept up to-date with the latest signature update. This allows the anti-virus software to detect the latest known viruses. It is recommended that the agents turn on automatic updates on their anti-virus software.
- Periodic full scan on system files and folders should be performed. This can be configured within the anti-virus software to run automatically.
- Agents should exercise caution before opening any email attachments and clicking on links received in emails, instant messenger or social media websites as they may be used to compromise the device.

[2] Agents should check the manufacturer website on the version of the OS and software that is still supported.

3.5 Network Controls

- Agents should enable the Firewall features that are normally bundled with their anti-virus software.
- The default Firewall feature within the OS should also be enabled.
- Agents should not use untrusted public wireless network to send customer data or payment information as they may not be secured.

3.6 Multi-factor Authentication

- Although it is not always possible to enable multi-factor authentication on laptop or desktop, Agents should do so where possible to secure the device that they are using.

4. Appendix

4.1 Definition

This section defines some terms used in the Guidelines.

No	Term	Definition and Comments
1	Insurance agent	As defined in the Insurance Act (Chapter 142) section 1A: *(a)* a person who, as an agent for one or more insurers (which may include a foreign insurer carrying on insurance business in Singapore under a foreign insurer scheme), is or has been carrying on the business of — (i) receiving proposals for, or issuing, policies in Singapore; (ii) collecting or receiving premiums on policies in Singapore; or (iii) arranging contracts of insurance in Singapore; or (*b*) a person who acts for, or by arrangement with, a person referred to in paragraph (*a*) in the performance of all or any of the activities carried out by the person referred to in paragraph (*a*), but does not include such persons or class of persons as the Authority may prescribe
2	Customer	A customer or prospective customer of an insurer or insurance agent, or an insured or prospective insured of an insurance policy
3	Virus definition file	A file created by the anti-virus vendor to inform the anti-virus software of new viruses and the detection mechanism
4	Encryption	To protect the data by converting the data, using a mathematically formula, into another form that is not easily understood to prevent unauthorised access
5	Cloud-based storage	Internet-based storage where the physical location of the storage is not known
6	Data destruction software	A software or application that is designed and developed for the objective of securely erasing electronic data
7	Jail-broken device	Typically associated with an iOS device where the software and security restrictions imposed by iOS are removed
8	Rooted device	Typically associated with an Android device modified to enable the user to run/operate the device with privileged rights
9	Bitlocker	BitLocker is a full disk encryption feature included with Windows Vista and later. It is designed to protect data by encrypting entire disc volumes.