Life Insurance Association Singapore
LIFE IS WORTH PROTECTING. INVEST IN IT.

GENERAL INSURANCE ASSOCIATION

Data Loss Protection Guidelines

For Insurance Agents

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

6 February 2017

Change History

Version	Change Description	by	Date
1.0	Initial Official release	ISCCS	6 Feb 2017

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 best practices for managing and handling sensitive information and promote the adoption of these best practices.

2. Applicability of the Guidelines

- The Guidelines are standards of industry best practices for insurance agents.
- The Guidelines apply to all devices 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.

3. Guidelines on Laptop / Desktop Protection

3.1 Virus / 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.
- Periodic full scan on system files and folders should be performed.

3.2 Operating System ("OS") and Software Patching

- Security patches for OS and software installed on laptops and desktops should be implemented at the earliest possible time.

3.3 Password Management

- Passwords should be made up of alphanumeric characters.
- Passwords should be at least eight characters long.
- Passwords should be changed periodically.
- Previously used passwords should not be reused for a period of time.

3.4 Data Protection

- Laptop or desktop hard disk containing customer data should be encrypted[4].
- Customer data or payment information should be encrypted before storing on or backup to any storage media including portable storage devices and cloud-based storage[5].
- Customer data or payment information should be securely erased using data destruction software[6] before disposal of the laptop / desktop.

4. Guidelines on Mobile Devices Protection

- Software with remote wipe capability should be installed and enabled on the mobile devices (e.g. smart phones or tablets).
- Mobile devices should not be jail-broken[7] or rooted[8].
- Device password should be enabled on mobile devices.
- Device password should be changed periodically.
- Security patches for mobile OS and applications should be installed or upgraded to the latest version at the earliest possible time.

- Customer data or payment information should be encrypted before storing on or backup to any storage media or cloud-based storage.

5. Suggestions to Implement the Guidelines

This section provides some suggestions to help insurance agents in meeting the recommendations in the Guidelines.

No	Data Loss Protection Control	Suggestions
A. Guidelines on Laptop/ Desktop Protection		
1. Virus / Malware Protection		
1.1	Anti-virus software should be installed	• *Insurance agents can install anti-virus software that are recommended by insurers*
1.2	Anti-virus software and virus definition files should be kept up to-date with the latest signature update	• *Insurance agents can turn on automatic updates on their anti-virus software*
1.3	Periodic full scan on system files and folders should be performed	• *Insurance agents can configure full virus scan to run periodically*
2. OS and Software Patching		
2.1	Security patches for OS and software installed on laptops and desktops should be implemented at the earliest possible time	• *For laptops and desktops running Windows, insurance agents can turn on "Automatic update" in the control panel. For MacBook, insurance agents can download updates from the AppStore periodically*
3. Password Management		
3.1	Passwords should be made up of alphanumeric characters	• *An example of a good password is: S0tj!690a*
3.2	Passwords should be at least eight characters long	
3.3	Passwords should be changed periodically	• *It is recommended to change password every 3 months*
3.4	Previously used passwords should not be reused for a period of time	• *It is recommended not to reuse a password for at least 10 password*

No	Data Loss Protection Control	Suggestions
		change cycles
4. Data Protection		
4.1	Laptop or desktop hard disk containing customer data should be encrypted	• *Insurance agents can use Windows Bitlocker[9] to encrypt laptop or desktop hard disk. Alternatively, insurance agents can use third party encryption software recommended by insurers to encrypt the hard disk.*
4.2	Customer data or payment information should be encrypted before storing on or backup to any storage media including portable storage devices and cloud-based storage (e.g. *Dropbox, OneDrive, iCloud, etc.)*	• *Insurance agents can either encrypt the storage media, or encrypt each record/file*
4.3	Customer data or payment information should be securely erased using data destruction software before disposal of the laptop / desktop	• *Insurance agents can use data destruction software recommended by insurers to erase the data stored on the hard disk*
B. Guidelines on Mobile Devices Protection		
5. Mobile Device Management		
5.1	Software with remote wipe capability should be installed and enabled on the mobile devices (e.g. smart phones or tablets)	• *iPhone users can enable the "find my phone" feature on iOS* • *Android users can turn on "Android Device Manager" under device setting*
5.2	Mobile devices should not be jail-broken or rooted	
5.3	Device password should be enabled on mobile devices	
5.4	Device password should be changed periodically	
5.5	Security patches for mobile OS and applications should be installed or upgraded to the latest version at the earliest possible time	• *For iOS devices, insurance agents can download and install OS or application updates from the AppStore.*
5.6	Customer data or payment information should be encrypted before storing on or backup to any storage media or cloud-based storage	• *Insurance agents can either encrypt the storage media, or encrypt each record/file*

6. Appendix

6.1 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.