

**WRITTEN VOLUNTARY UNDERTAKING (“Undertaking”)  
TO THE PERSONAL DATA PROTECTION COMMISSION**

This Undertaking is given to the Personal Data Protection Commission or its delegates pursuant to section 48L(1) of the PDPA, by:

**Equity Solution Pte Ltd**

UEN: 201601961Z

Registered Address: 16 Kallang PI #07-03 Singapore (339156)

(hereinafter referred to as the “**Organisation**”).

By signing this Undertaking, the above-named Organisation acknowledges the matters stated herein and undertakes to the Commission in the terms set out herein.

**1. DEFINITIONS**

1.1 In this Undertaking:

- (a) “**PDPA**” means the Personal Data Protection Act 2012 (No. 26 of 2012); and
- (b) “**Relevant Provisions**” means the provisions in Parts 3, 4, 5, 6, 6A, 6B and 9, and section 48B(1) of the PDPA.

**2. ACKNOWLEDGEMENTS**

2.1 The Organisation hereby acknowledges the following matters:

- (a) The Commission has carried out investigations into certain acts and practices of the Organisation, and has reason to believe that the Organisation has not complied, is not complying, or is likely not to comply with one or more of the Relevant Provisions. The relevant facts and circumstances are summarised at Schedule A.
- (b) As a result of any non-compliance with the PDPA by an organisation, the Commission has a number of enforcement options under the PDPA, including the option to issue directions under sections 48I or 48J of the PDPA.

(c) The Commission recognises that the Organisation has made efforts to address the concerns raised in this case and to improve its personal data protection practices. In addition, the Organisation was cooperative in the course of the investigation and was responsive to requests for information. The Commission further recognises that the Organisation appears ready to implement or is in the midst of implementing the steps set out in Schedule B.

(d) Having carefully considered all the relevant facts and circumstances, the Commission takes the view that this is an appropriate case in which an Undertaking may be accepted.

2.2 The Organisation also acknowledges and agrees that the Commission may publish and make publicly available this Undertaking, and without limitation to the foregoing, the Commission may issue public statements referring to this Undertaking and/or its contents in whole or in part.

### **3. UNDERTAKINGS**

3.1 The Organisation undertakes that it has taken, or will take all necessary steps, to carry out the actions or refrain from carrying out the actions referred to in Schedule B, and where applicable, in accordance with the stipulated timelines.

### **4. COMMENCEMENT**

4.1 This Undertaking shall take effect upon the acceptance by the Commission of the Organisation's duly executed Undertaking.

### **5. THE COMMISSION'S STATUTORY POWERS**

5.1 In order to provide the Organisation with an opportunity to complete all necessary steps to implement its undertakings set out in clause 3 above, the Commission will exercise its powers under section 50(3)(ca) of the PDPA to suspend the investigations referred to in clause 2 on the date the Undertaking takes effect as set out in clause 4.1.

5.2 The Organisation acknowledges that the Commission will verify the Organisation's compliance with its undertakings set out in clause 3 above, and if necessary, will exercise its powers under the Ninth Schedule of the PDPA to do so.

5.3 Clause 5.1 above shall be without prejudice to the Commission's statutory powers to conduct or resume, at any time, the investigations referred to in

clause 2 above if it thinks fit, including but not limited to the situation where the Organisation fails to comply with this Undertaking or part thereof in relation to any matter.

5.4 Nothing in this Undertaking, including the Commission's acceptance of the Undertaking, is intended to, or shall, fetter or constrain the Commission's rights and statutory powers (including but not limited to those under sections 48I, 48J, 48L(4) and 50 of the PDPA) in any manner. Neither shall be construed as creating any anticipation or expectation that the Commission will take or not take any particular course of action in the future (whether in the present case or in respect of any other case concerning a breach or suspected breach of the PDPA). The acceptance of this Undertaking is strictly confined to the particular facts of the present case, and is made on the basis of the representations and information provided by the Organisation. The acceptance of an Undertaking in this case shall not be construed as establishing any precedent.

## 6. VARIATION

6.1 This Undertaking may be varied only with the express written agreement of the Commission.

This document has been electronically signed. The Parties hereby affirm that the electronic signatures have been affixed with the due authorisation of each Party and that Parties intend for the electronic signatures to carry the same weight, effect and meaning as hand-signed wet-ink signatures.

SIGNED, for and on behalf of )

**Equity Solution Pte Ltd** )

By the following: )

Name: \_\_\_\_\_ )

Designation: \_\_\_\_\_ )

Date: \_\_\_\_\_ )

ACCEPTED by \_\_\_\_\_ )

)

Name: \_\_\_\_\_ Yeong Zee Kin \_\_\_\_\_ )

Designation: Deputy Commissioner / Commissioner

Personal Data Protection \_\_\_\_\_ )

Date: \_\_\_\_\_ )

# **SCHEDULE A**

## **SUMMARY OF FACTS**

1. On 3 February 2021, the Organisation was subjected to a phishing attack after a staff opened an email containing an excel file with a macro-enabled malware.
2. As a result of the attack, the personal data of the Organisation's approximately 1,359 users including their name, residential address, date of birth, NRIC numbers, passport numbers and financial information were affected.

# SCHEDULE B

Remediation Plan	Status	Date of Completion
<p><b>Remedial Actions Taken in Response to the Incident</b></p> <p>The following are the remedial actions which had been adopted in response to the Incident:</p> <p>(1) ES has changed its passwords of the affected email account on 19 February 2021.</p> <p>(2) ES engaged CS Intelligence to conduct a scan on the compromised laptop to ensure that there are no traces of any malware or malicious files.</p> <p>(3) ES has deleted all email containing personal data or attachments with personal data from the inbox and sent folder of the affected email account on 22 February 2021.</p> <p>(4) ES has stopped the use of cloud storage services and migrated all the electronic files containing personal data into an external hard drive.</p> <p>(5) The external portable hard drive will be stored securely in a locked drawer in the office when not in use.</p>	Completed	February 2021
<p><b>Securing Files and Documents using Password Protection</b></p> <p>ES will move password protect all of its electronic files containing personal data of its customers when transmitting it by way of email and require that all of its business partners to do the same. The password to the files will be sent in a separate email. This is to reduce risk of ES falling victim to phishing emails and mitigate the risk of data exfiltration. This policy change will be reflected in ES's DPMP.</p>	Completed	February 2021
<p><b>Hardening of Operating System</b></p> <p>(1) ES will ensure that the windows OS firewall is activated and updated to deny unauthorised inbound connection and only allow approved outbound connection.</p> <p>(2) ES will remove and disable non-essential software, drivers, services, file sharing, and functionality which could act as back doors to the system.</p> <p>(3) ES will turn on the HDD encryption, such as windows BitLocker, to prevent any data exfiltration</p>	Completed	February 2021

<p>in the event the computer were to be stolen or when there is a HDD replacement</p> <p>(4) ES will subscribe to a managed service provider (MSP) with 24x7 protection by Security Operation Centre provided by CS Intelligence (CSI) to monitor and protection against potential malicious activities. The CXO will be installed on the company laptops to safeguard the computers from advance malware that does keylogging activities, ransomware, code injections and other potentially malicious acts. A copy of the promotional material for the CXO package is annexed hereto.</p>		
<p><b>Implementing Strong Password Protection Policy</b></p> <p>ES will require its employees to change their login credentials for both their laptops and email accounts regularly every month using a complex password combination. All passwords must contain at least 1 uppercase alphabet, 1 lowercase alphabet and 1 special symbol.</p>	Completed	February 2021
<p><b>Reviewing and Updating Email Usage Policy</b></p> <p>The inbox and sent folder of ES email accounts will be reviewed once every 6 months for emails containing personal data or email attachments containing personal data. Such emails and/or email attachments will be password protected and archived in ES's offline external portable hard drive to be kept in a secured locked drawer/safe and deleted from the inbox and/or sent folder once the transaction or the matter to which they relate have concluded.</p> <p>ES will also review its email account access logs regularly to detect if there is suspicious login outside of Singapore.</p>	Completed	February 2021
<p><b>Implementing Training and Awareness Programme for Employees</b></p> <p>User training awareness will be implemented to be more vigilant and learn how to identify legitimate email without clicking on any unknown or suspicious emails.</p> <p>A refresher course will also be carried out for its employees on the PDPA obligations, as well as inform them of the company's updated data protection policies and processes.</p>	Completed	May 2021

<p><b>Reviewing and Updating Personal Data Protection Policy</b></p> <p>A review of the company's policies and processes will be conducted by compiling and supplementing existing personal data protection policies and processes into the company's Data Management Programme (DPMP).</p>	Completed	May 2021
<p><b>Subscribing to Reputable Email Service Provider</b></p> <p>ES will change its email hosting service provider from Vodien to Microsoft Office which provides greater privacy and security features to prevent unauthorised access, such as two-factor authentication logins, as well as anti-spam, anti-malware, and anti-phishing features to scan and flag out emails with potentially malicious file attachments. In particular, Microsoft has an implicit email authentication built in which verifies that email messages from a sender are legitimate and come from expected sources.</p> <p>Once ES has changed its email hosting service provider, ES will turn on its two-factor authentication as a secondary authentication to all of its email addresses to prevent unauthorised access to the accounts.</p> <p>ES would also be enquiring on other email hosting service provider such as google, adnovum, bluehost and godaddy for such purposes.</p>	In progress	July 2021
<p><b>Data Security Enhancement:</b></p> <p>Data would be transferred to a Seagate external hard drive which is equipped with password protection and AES-256 hardware encryption to prevent data exfiltration in the event that the external hard drive is lost.</p> <p>The external portable hard drive will be stored securely in a locked drawer in the office when not in use.</p>	In progress	July 2021