

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

This Undertaking is given to the Info-communications Media Development Authority designated as the Personal Data Protection Commission under section 5(1) of the PDPA (hereinafter referred to as the “**Commission**”), by:

DLI Asia Pacific Pte Ltd
UEN: 201431235K
Registered Address: 12 Marina view #24-03/04 Asia Square Tower 2
S(018961)

(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) “**Commission’s Letter**” means the letter dated 1 December 2020 from the Commission to the Organisation, concerning its investigation under the PDPA, including the appendices thereto;
- (b) “**Data Protection Provisions**” means the provisions in Parts III to VI of the PDPA; and
- (c) “**PDPA**” means the Personal Data Protection Act 2012 (No. 26 of 2012).

2. ACKNOWLEDGEMENTS

2.1 The Organisation hereby acknowledges the following matters:

- (a) As referenced in the Commission’s Letter, the Commission has carried out investigations into certain acts and practices of the Organisation, which potentially infringe one or more of the Data Protection Provisions.
- (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 give a direction under section 29 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 the remediation plan set out in clause 3 below forthwith.

- (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 (which to avoid doubt, includes the Commission's Letter), 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 implement its remediation plan, namely, to carry out the actions referred to in Schedule A in accordance to 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) 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.
- 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 section 29 and section 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 by Info-communications Media Development Authority and **DLI Asia Pacific Pte Ltd**. 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)

DLI Asia Pacific Pte Ltd)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED, for and on behalf of)

Personal Data Protection Commission)

By the following:)

Name: _____)

Designation: Deputy Commissioner
for Commissioner for Personal Data Protection)

Date: _____)

SCHEDULE A

Item	Status	Date of Completion (Month-Year)
<p>Implement Multi-Factor Authentication to Strengthen VPN Login</p> <p>Multi-factor Authentication (MFA) will be implemented to further strengthen VPN login. Remote VPN access will be authenticated with an additional factor on top of the current 2FA controls already in place.</p>	In Progress	Dec-20
<p>Implement Different User Accounts for VPN and Server Access</p> <p>Setup different User Id or Account for VPN & Server Access to further strengthen login controls, preventing use of same ID & Password to access both the VPN and Server Systems.</p>	Completed	May-20
<p>Implement Virtual Desktop for IT Vendor with Activity Monitoring</p> <p>Virtual desktop will be implemented for IT Vendor Access & Monitoring to further strengthen vendor support access controls. IT Vendors are only allowed access to System using Virtual Desktop to better secure access, and such access is monitored.</p>	In Progress	Jan-21
<p>Engage Security Consultant to Review Current Setup</p> <p>Conduct survey and review requirements of current IT Infrastructure & Systems setup to further enhance protection against cyber-attacks.</p>	In progress	Jan-21
<p>Implement Additional Security Monitoring</p> <p>Review requirements of additional security monitoring by another security company in addition to the current IT vendor to have a "Check & Balance" mechanism to ensure that the current IT vendor</p>	In Progress	Dec-20

<p>carries out its obligations to implement any security patches for the following systems:</p> <ul style="list-style-type: none"> • Firewall • VPN Server • Domain Controller 		
<p>Patch Update & Management Improvement</p> <p>Review current Patch Update & Management and request IT vendor to improve its processes to ensure timely updates for system patches, specifically where there are high priority and critical patches which are published</p>	Completed	Oct-20
<p>Remedial Actions Taken in Response to the Incident</p> <p>The following are the remedial actions which had been put in place in response to the incident:</p> <ol style="list-style-type: none"> 1) Change all passwords for all users and administrators 2) Re-format all suspected laptops that potentially could have been compromised as advised by the Forensic company. Total 34 laptops re-formatted. 3) Closed communication to Dark Web on the Firewall. 4) Turned off the compromised VPN server once we confirmed that it had been compromised. 5) Check & confirm the version of the second VPN server to make sure that it is updated to the latest version. 6) Conduct a scan on all servers and laptops deployed to ensure that there are no traces of the ransomware files, or malware. 7) Stop the use of the shared folder/files in the File Server by all users, and to migrate all shared folders for better controls. 	Completed	May-20
<p>Fundamental Reform of File Management</p> <p>Establish thorough file management rules in the cloud:</p>	Completed	Aug-2020

<ul style="list-style-type: none"> 1) Thorough implementation of customer information handling and reporting rules 2) Remove unnecessary personal information promptly 3) Passwords implemented to secure & protect all files that has personal information in limited access folder 4) Store all files with personal information in limited access folder 		
<p>Implementing Email Rules (Internal & External)</p> <ul style="list-style-type: none"> 1) Checking of receiver address, passwords, contents of Emails and files 2) Password rules for attachments 3) Strengthening of password rules 	In Progress	Jul-2020
<p>Others</p> <p>Implement compliance trainings</p>	Completed	<p>Jun-2020</p> <p>Jul-2020</p> <p>Aug-2020</p>
<p>Review of internal policies relating to handling of personal information to align with PDPA amendments</p>	In progress	Mar-2021