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:

Pu Tien Restaurant Pte Ltd
UEN: 200001660W
Registered Address: 127 Kitchener Road, Singapore 208514

(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

In this Undertaking:

(a) "**PDPA**" means the Personal Data Protection Act 2012; and

(b) "**Relevant Provisions**" means the provisions in Parts III, IV, V, VI, VIA and IX, 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

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

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

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)

PU TIEN RESTAURANT PTE LTD)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED by)

)

Name: _____)

Designation: Deputy Commissioner

Personal Data Protection)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. The Personal Data Protection Commission (the "Commission") was notified by Pu Tien Restaurant Pte Ltd (the "Organisation") on 6 December 2021 that it was subject to a ransomware attack on 24 November 2021. A threat actor used stolen administrator account credentials to enter the Organisation's network through a remote desktop protocol port. As a result, its servers containing personal data were accessed and encrypted by ransomware.

2. 350 employees' personal data were encrypted. The personal data included full names, contact numbers, NRIC, work permit, passport numbers, birth certificate and education certificate images, and bank account numbers. The Commission noted that there was no evidence of exfiltration of the personal data.

3. To prevent a recurrence of a similar incident, the Organisation took immediate remedial action to address the cause of the personal data breach.

SCHEDULE B

Accountability – Governance, Policies and Procedures

S/N	Remediation Step	Completion Date/ Target Completion Date
1.	Appoint a Data Protection Officer	Completed in May 2022
2.	Develop an IT Security policy comprising • Secure management of accounts and passwords, user authentication, management of physical access to assets • Authorisation process to onboard new hardware and software	Completed in June 2022
3.	Develop cyber hygiene practices and guidelines for employees to adopt in their day-to-day operations	To be completed by January 2023
4.	Develop and implement practices and guidelines on how data is managed securely, including • Protection of data • Prevention of leakage of data by employees • Secure disposal of data	To be completed by Q1 2023
5.	Develop and implement practices and guidelines on incident response	To be completed by January 2023

Staff Training and Communications

S/N	Remediation Step	Completion Date/ Target Completion Date
1.	Mandate the staff to complete the PDPA E-learning	To be completed by December 2022

S/N	Remediation Step	Completion Date/ Target Completion Date
2.	Identify and facilitate key personnel to attend PDPC courses (e.g. Fundamentals of the PDPA 2020)	To be completed by December 2022
3.	Provide cybersecurity awareness training for employees in the organisation, minimally covering these topics: • Protect yourself from phishing • Set strong passphrase and protect them • Protect your corporate and/or personal devices (used for work) • Report cyber incidents • Handle and disclose business-critical data carefully • Work onsite and telecommute in a secure manner	To be completed by January 2023

Data Security Practices

S/N	Remediation Step	Completion Date/ Target Completion Date
1.	Subscribe to MS365 Premium license and configured with • Microsoft Defender • MFA • Encryption • Appropriate folder permission in SharePoint	Completed in December 2021
2.	Install an on-premise server with Hybrid connectivity to cloud servers and to configure access control on • Password policy • Network control limitation • Windows patches update • File transfer encryption	To be completed by September 2022

S/N	Remediation Step	Completion Date/ Target Completion Date
3.	Configure data encryption in transit for: • HTTPS secure internal web access • SFTP (for POS system file transfer) • Change of Port access	Completed in June 2022
4.	Subscribe to TrendMicro Cloud Security with the following configurations: • Daily routine scanning of viruses and malware • Network access limitation • Daily updates to signature files to detect new malware	Completed in May 2022
5.	Subscribe to FortiGate UTM Firewall service with proper configuration of policy and network security.	Completed in July 2022 Penetration test to be conducted by November 2022
6.	Implement secure configuration for hardware and software assets, including • Enforcing security configurations or enabling security features for assets and avoiding or updating weak configuration • Replacing or upgrading insecure configurations and weak protocols • Turning off features/services that are not used	To be completed by Q1 2023
7.	Install Windows Server update service to push critical update to end user devices	To be completed by September 2022
8.	Subscribe to Acronis Cloud backup and configured with daily incremental backups and weekly full backups	To be completed by October 2022

Review

S/N	Remediation Step	Target Completion Date
1.	Ensure that the latest software updates installed on devices and systems	To be completed by Q1 2023
2.	Carry out review and update of: • Data protection and security policies • Configuration settings for hardware and software • Use accounts to ensure all accounts are active and the rights assigned are necessary • Incident response plan	To be completed by November 2022
3.	Conduct a refresher on cyber and data protection awareness training for key employees on handling personal data.	To be completed by Q1 2023
4.	Conduct phishing simulation exercises to train the employees to be alert.	To be completed by Q1 2023
5.	Conduct table-top exercise to test the cyber and data breach response plan.	To be completed by December 2022
6.	Audit on sharing of passwords such as admin credentials, displaying post-it notes of password publicly or storing passwords in public web folders.	To be completed by November 2022
7.	Ensure that regular backups are set up according to the backup policy. Backup media regularly tested to ensure that the backup data can be recovered and restored.	To be completed by October 2022