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:

Tat Hong Heavyequipment (Pte.) Ltd.
UEN: 197801297W
Registered Address:82 Ubi Avenue 4
#05-01
Edward Boustead Centre
Singapore 408832

(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)

Tat Hong Heavyequipment (Pte.) Ltd.
)

By the following:)

Name: ____)

Designation: ___________________________________)

Date: ____)

ACCEPTED by)

)

Name: ______________________________)

Designation: Deputy Commissioner
Personal Data Protection)

Date: ______________________________)

SCHEDULE A

SUMMARY OF FACTS

1. On 11 July 2022, the Organisation was subjected to a ransomware attack in which various systems within the Organisation's network were encrypted. A total of 43 virtual machines, 4 physical servers, 3 employees' PC and network attached storge were affected. The threat actor had likely gained access to the Organisation's network by exploiting an open Microsoft Remote Open Desktop protocol to a UAT server.

2. As a result, the personal data of the Organisation's 3,377 current and former employees and their next-of-kin may have been compromised. The personal data included names, dates of births, NRIC/FIN/Passport numbers, addresses, contact numbers, bank account numbers (for crediting of salaries) and fingerprints (for door access). There was no evidence of personal data exfiltration and all personal data have been fully restored.

3. The Organisation took immediate remedial actions to address vulnerabilities, to prevent a recurrence of a similar incident.

SCHEDULE B

Remediation Plan	Status	Target Date of Completion
Network Security and Design		
1) Hardening of the Perimeter Firewall. Fine tune Firewall Configuration / Settings to prevent malicious traffic from outside from gaining access to the Internal Network. a) b) c) REDACTED FOR CONFIDENTIALITY	Completed	Aug 2022
2) To ensure effective controls are current and remain in place periodic Vulnerability Assessment and Penetration Testing will be done at least annually or after major systems upgrade/enhancement.		
a) Initial Vulnerability Assessment to assess the current state of our systems was conducted and form the basis of the remediation process.	Completed	Aug 2022
b) Pre-commissioning Penetration Testing will be conducted after all the major changes system changes/enhancements are completed to validate effectiveness of the current upgrades/enhancements.	Scheduled	Nov 2022
3) Engage third party security company to conduct security traffic monitoring and firewall rules review as well as vulnerability assessment to assess and rectify security deficiency and inefficiency and propose relevant rectification works.	Completed	Aug 2022
4) Get Additional Modules to enhance the capability of the Perimeter firewall.	In progress	Sep 2022

a) Advance URL Filtering – manage users web access. b) DNS Security – protect against malware that abuses DNS for malicious activity. c) Wildfire – delivers inline machine learning to prevent never-before-seen file and web-based threats.		
5) Engage Cyber-security expert to assist IT Staff and Company to enhance its security posture, compliance with regulatory requirements and to jumpstart the level of cybersecurity knowledge in company.	Completed	Aug 2022
6) Assigning static IP addressing for critical/high risk computers. All servers are using static IP addressing already.	Completed	Aug 2022
7) Additional physical server backup process that will be connected to the server farm during backup process and will be disconnected to the network after successful backup.	Completed	Aug 2022
8) Redesign network so that all traffic will pass through the main firewall for better visibility, monitoring and logging. a) b) c) REDACTED FOR CONFIDENTIALITY d) e)	In progress	Oct 2022

Identity and Access Management		
9) Identity and Access Management a) Enforced enhanced password policy. b) Change Domain Administrators password. c) Randomized server local administrator password. d) Force Domain users to change their password and adhere to the enhanced password policy. e) Forced change of users email password. f) Clean up the AD - retaining only active users and machines and review access control.	Completed	Aug 2022
10) Implement Multi-Factor Authentication for privileged accounts and high-risk connections.	In progress	Oct 2022
Endpoint Security		
11) Ensure that all active PC and server are installed with Endpoint Detection and Response (EDR) a) Update all PC/Servers to the latest patch and definition of EDR + AV application. b) Update all PC/Servers with the latest windows update. c) Update/replaced outdated applications and operating system.	Completed	Aug 2022
12) Upgrade advance EDR + AV application to replace the existing EDR + AV to include advance features such as machine learning and threat hunting.	In progress	Nov 2022
13) Measures against lateral movements and unauthorised changes. Related measures to reduced potential attack surface for lateral movement via a combination of windows policy and EPP/MDR solutions.	Scheduled	Nov 2022

a) Remove unnecessary access to administrative shares where applicable and/or restrict admin shares to privileges to only necessary services or user accountsand perform continuous monitoring for anomalous activity using EPP/MDR. b) Ensure that upgraded EDR or have separate host-based firewall to only allow connections to administrative shares via server message block (SMB) for a limited set of administrative machines. c) Enabled protected files in the operating system to prevent unauthorised changes to the critical files. d) Disable Command line and scripting activities and permissions whenever possible and to allow restrictive access to only required machines as fully disabling the features would inhibits legitimate and productive uses of the command lines and scripting.		
14) Enhance Cybersecurity Platform to improved security posture by implementing Managed Detection and Response (MDR) a) Using security expert to manage, monitor and respond to threats. b) Provides visibility across assets. c) Provide threat detection and real time prevention of identity based attack. d) Provide continuous, comprehensive visibility to endpoint activity. e) Protect against malware and malware-free threats. f) Managed threat hunting to stops hidden, advanced attacks.	Scheduled	Nov 2022

Data Security		
15) Purge Ex-Staff record in HR Server according to data retention policy.	In progress	Sep 2022
16) Upgrade existing HRMS that complies with latest Industry standard encryption algorithm.	In progress	Dec 2022
17) Data minimisation across all data stores. Full backup of personal datasets are done daily. a) Limit the backup data retention to 31 days and any back up older than 31 days will be purged automatically.	Scheduled	Nov 2022
People Management		
18) End-user Awareness Training a) Conduct end user awareness training such as phishing simulation exercises to train employees and IT staff to identify phishing emails and be alert to spot signs of compromise. b) Be able to spot email impostor scam (Spoofing) and how to react to it.	In progress	Oct 2022