VOLUNTARY UNDERTAKING UNDER
SECTION 48L OF THE PERSONAL DATA PROTECTION ACT 2012

Case number: DP-2305-C1003

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Sunray Woodcraft Construction Pte Ltd (UEN No. 198703016K)

… Organisation

The Commission has reasonable grounds to believe that the Organisation has not complied, is not complying or is likely not to comply with section 24 of the Act. In order for the Commission to suspend its investigation pursuant to section 50(3)(ca) of the Act, the Organisation HEREBY UNDERTAKES that it will:

(a) Complete the remediation plan set out at Schedule B within the timelines stated in Schedule B; and

(b) Within 14 days of the completion of the remediation plan set out at Schedule B, provide the Commission with a copy of the declaration set out at Schedule C duly signed by the signatory of this Undertaking or a representative of the Organisation of equal designation.

The Organisation acknowledges that the Commission shall be entitled to publish and make available to the public this Undertaking and the summary of the Commission's findings set out at Schedule A to this Undertaking.

The terms of this Undertaking may be varied by the written agreement of the Commission and the Organisation.

SIGNED, for and on behalf of)

Sunray Woodcraft Construction Pte Ltd)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 11 May 2023, the PDPC was notified by Sunray Woodcraft Construction Pte Ltd ("**SWCPL**") of a ransomware attack on its servers on or about 25 April 2023 causing loss of access to IT systems and encryption of files with personal data.

2. As a result, the personal data of 2,130 individuals including their names, addresses, personal email addresses (in respect of 689 individuals), telephone numbers, NRIC numbers, passport numbers, photographs, dates of birth, bank account numbers and salary information was affected.

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

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
Technical remediation			
1	Exploitable vulnerabilities in software used.	Software in use will be updated to the latest version available.	Completed
2		SWCPL will evaluate and thereafter implement/deploy technological measures to ensure that software on all devices is updated as new patches become available.	December 2023
3		SWCPL will conduct a risk assessment for software that cannot be updated (e.g., because it is needed for compatibility with legacy hardware such as CNC machines / laser cutters), to evaluate vulnerabilities, threats, impacts, mitigation measures, business context, compliance, and risk acceptance to inform decision-making and appropriate prioritization of resources for effective risk management.	December 2023
4	Lack of enforcement of multi-factor	SWCPL will enforce multi-factor authentication for all	Completed

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
	authentication for virtual private network access.	account logins for VPN connections to its IT systems.	
5	Inadequate maintenance of security software (e.g. antivirus, firewalls).	SWCPL will update all security software to the latest version available, including updating antivirus patterns.	Completed
6		SWCPL will evaluate and thereafter implement/deploy technological measures (such as vulnerability scanning engines) to ensure that security software is updated as new patches become available.	December 2023
7		SWCPL will conduct a thorough firewall rules review to ensure adequate protection for SWCPL. Any issues identified will be resolved.	Completed
8		To strengthen SWCPL's security defense, SWCPL is evaluating and will deploy intrusion detection systems (IDS), intrusion prevention systems (IPS), or endpoint detection and response (EDR) to strengthen its	SentinelOne (an EDR) has already been deployed. IDS/IPS will be managed through our Palo Alto firewall, which has already been deployed. Continuous evaluation and fine

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
		cybersecurity profile. SWCPL will also perform continuous evaluation and fine-tuning of IDS. IPS, and EDR.	tuning will be performed as necessary.
9	Use of default usernames for high-privilege accounts.	SWCPL will change usernames for high-privileged accounts that are default usernames. Technological policies will be implemented to ensure that default usernames (e.g. “admin” or “user”) are not used.	Completed
10	Weak enforcement of secure passwords.	SWCPL will strengthen password enforcement by implementing Group Policy Object (GPO) policies that enforce compliance with SWCPL's password policy on complexity, length, and expiry.	Completed
11	Account lockout policies	SWCPL will enforce automatic account lockout policies which will lockout an account after 5 failed login attempts.	Completed
12	On-premises backup dependency increases vulnerability to data loss or unavailability during	SWCPL will evaluate and thereafter implement of off-site	Evaluation will be completed by November 2023. Actual backups will be

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
	disasters or cyber-attacks.	back tape backup or cloud-based backup	performed as necessary.
13	Implementation of centralized logging capabilities to ensure that system logs are available in the event of a cyber incident.	SWCPL will evaluate and thereafter implement systems to retain and adequately secure logs from network devices, local hosts and cloud services, etc for at least 90 days.	November 2023
Policies / Process Remediation			
14	Strengthen incident response plan.	SWCPL will draft an Incident Response Plan that includes an outline of the scope, incident response methodology, incident response phases, guidelines for the incident response process, and documentation, tracking, and reporting procedures, ensuring a comprehensive and tested approach to addressing information security incidents.	November 2023
15	Vulnerability testing	SWCPL will research available vulnerability testing solutions to conduct a suitable penetration test after the abovementioned steps.	Research on vulnerability testing solutions will be completed by November 2023. Penetration testing will

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
		SWCPL will also implement periodic penetration testing.	be conducted as needed.
16	Implementing asset management actions to ensure that information about SWCPL's IT assets are available and accurate.	SWCPL will implement the following asset management actions: 1. Keep an inventory of hardware and software assets to identify outdated hardware and software. 2. Keep an inventory of user accounts. 3. Maintain an updated network diagram of SWCPL's network.	Items 1 and 2: November 2023 Item 3: Completed. SWCPL is actively maintaining this network diagram.
17	Implementing account management actions to ensure security of user accounts	SWCPL has in place the following account management actions. 1. Implementing procedures and processes to perform periodic review of user accounts and removal of inactive accounts.	Item 1: SWCPL already has in place such procedures and processes. SWCPL will regularly review these procedures and processes to ensure that they are complied with. Item 2: Completed. SWCPL will regularly review these procedures and

No.	Potential Risk Factors / Improvement Areas	Remediation Plan	Target Completion (Date)
		2. Enforcing the principle of "least-privilege" to control user access rights.	processes to ensure that they are complied with.
18	Implementing written policies/processes/guidelines relating to the collection, use, disclosure, protection and retention of personal data in the possession and/or custody of SWCPL and/or its employees.	SWCPL will review and update its internal policies/processes relating to the collection, use, disclosure, protection, and retention of personal data in the possession and/or custody of SWCPL and/or its employees, including but not limited to ensuring the proper documentation of the policies and processes and enhancing training for all staff on their data protection.	November 2023

SCHEDULE C

Case number: DP-2305-C1003

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Sunray Woodcraft Construction Pte Ltd (UEN No. 198703016K)

… Organisation

DECLARATION

I refer to the voluntary undertaking dated [_____] given by the Organisation to the Personal Data Protection Commission pursuant to section 48L of the Act ("**the Undertaking**").

I declare that the remediation plan set out at Schedule B of the Undertaking has been completed.

I acknowledge that by making a false declaration or providing false or misleading information to the Personal Data Protection Commission, I may be prosecuted for offences under section 51(3)(c) of the Personal Data Protection Act 2012 and/or section 182 of the Penal Code 1871.

_____ _____

Signature Date

_____ _____

Name Designation