

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 5
	Document Classification:	Internal
	Effective Date	10 June 2024
PHYSICAL & ADMINISTRATIVE SECURITY	Doc No	DPMP-PRO-09
	Revision	1.0

AMENDMENTS LOG

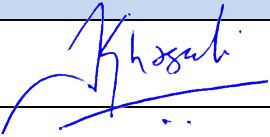
Revision History

Version	Date	Revision Author	Summary of Changes
1.0	10 June 2024	Edwin Soedarta DPO	First Release

Distribution

Name	Location
<i>All employees</i>	<i>Shared Folder</i>

Review & Approval

Name	Position	Signature	Date
Khasali M	Director		10 June 2024

THE SOFTWARE PRACTICE PTE LTD	No of Pages	2 of 5
	Document Classification:	Internal
	Effective Date	10 June 2024
PHYSICAL & ADMINISTRATIVE SECURITY	Doc No	DPMP-PRO-09
	Revision	1.0

Contents

AMENDMENTS LOG 1

RECORDS FOR DOCUMENT REVIEW 3

PURPOSE 4

SCOPE 4

RESPONSIBILITIES 4

PROCEDURES 4

1. Physical Security 4

2. Administrative Security 5

THE SOFTWARE PRACTICE PTE LTD	No of Pages	3 of 5
	Document Classification:	Internal
	Effective Date	10 June 2024
PHYSICAL & ADMINISTRATIVE SECURITY	Doc No	DPMP-PRO-09
	Revision	1.0

RECORDS FOR DOCUMENT REVIEW

To ensure the continuing suitability, adequacy and effectiveness of the documented information and its relevancy, a review of its contents should be conducted at a planned interval or when significant changes occur. The review should include assessing opportunities for improvement of the documented information and the approach to managing data protection in response to changes to the organization environment, business circumstances, legal conditions as well as the technical environment.

Instruction Guide:

Version 1.0, 2.0, 3.0... Version changed with amendments

Version 1.0 Version remained unchanged but update the last and next date of review

VERSION	REVIEW BY	DATE OF REVIEW	NEXT REVIEW DATE
1.0	Edwin Soedarta (DPO) Khasali M (Director)	10 June 2024	9 June 2025

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 5
	Document Classification:	Internal
	Effective Date	10 June 2024
PHYSICAL & ADMINISTRATIVE SECURITY	Doc No	DPMP-PRO-09
	Revision	1.0

PURPOSE

This document details the physical and administrative security measures employed by the organization to protect personal data.

SCOPE

This procedure applies to physical areas within the organization and security measures that all employees need to implement for data protection.

RESPONSIBILITIES

The Top Management has the prime responsibility and approval authority for this procedure.

The Data Protection Officer (“DPO”) together with the respective process owners are responsible to ensure implementation of the physical and administrative security measures detailed in this procedure within their area of responsibility.

PROCEDURES

The organization shall implement the following physical and administrative security arrangements to protect personal data in its possession or under its control.

1. Physical Security

- Mark confidential documents clearly and prominently. Personal data shall be classified and labeled as confidential.
- Store confidential documents in locked file cabinet systems.
- Only the data custodian can readily access the documents in locked file cabinet systems. Other employees’ access shall be restricted on a need-to-know basis and with proper authority.
- Confidential documents that are no longer needed (e.g., when ceasing the retention of personal data) shall be properly disposed of through shredding. Re-using of the papers shall not be allowed (e.g., putting confidential documents in recycle bin for re-printing). For shredding personal data on paper, the shredder to be used should be at least a level P-3 cross-cut shredder (instead of straight-cut shredder). For disposal of removable storage media and other details on secure disposal, refer to [DPMP-PRO-08 Data Retention & Destruction Process](#).
- Appropriate security measures to the office such as door entry control shall be implemented.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 5
	Document Classification:	Internal
	Effective Date	10 June 2024
PHYSICAL & ADMINISTRATIVE SECURITY	Doc No	DPMP-PRO-09
	Revision	1.0

2. Administrative Security

- Appropriate data protection and security responsibilities have been assigned to relevant employees in accordance with the Data Protection Management Programme Manual.
- Employees employed by the organization shall be bound by confidentiality obligations in their employment agreements.
- Employees shall acknowledge and comply with the established policies and processes in the organization's Data Protection Management Programmed (DPMP), with disciplinary consequences for breaches in line with DPMP-PRO-11 Compliance Monitoring & Violation Handling.
- The following shall be carried out to impart good practices in handling personal data and strengthen awareness of threats to security of personal data within the organization:
 - Training for new staff, existing staff and key employees with significant personal data protection obligations shall be provided in line with the Training Plan indicated in the Data Protection Management Programme Manual.
 - Communication programme shall be implemented as per Data Protection Management Programme Manual.
- Ensuring that employees and any third party engaged only hold appropriate amount of personal data necessary for the role and within their authority.
- Engagement of any third party for data processing shall follow the procedure DPMP-PRO-06 External Provider DDA & Evaluation.
- Compliance and monitoring activities shall be carried out in line with DPMP-PRO-11 Compliance Monitoring & Violation Handling.