

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	1 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	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

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	2 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

**Contents**

**AMENDMENTS LOG ..... 1**

**RECORDS FOR DOCUMENT REVIEW ..... 3**

**PURPOSE ..... 4**

**SCOPE..... 4**

**RESPONSIBILITIES AND AUTHORITIES ..... 4**

**PROCEDURE..... 4**

**1. MONITORING OF COMPLIANCE WITH POLICIES & PRACTICES..... 4**

**2. VIOLATION HANDLING..... 7**

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	3 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	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

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	4 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

## PURPOSE

The purpose of the procedure is to set out the process to regularly monitor compliance of practices with data protection policies in a structured and timely way.

The procedure also sets out enforcement and violation handling.

## SCOPE

This procedure applies to all the policies, practices and measures of the organization and to its employees.

Compliance with the data protection policies and requirements by third parties engaged by the organization shall be carried out in line with DPMP-PRO-06 External Provider Due Diligence Assessment & Evaluation.

## RESPONSIBILITIES AND AUTHORITIES

The 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 assess, investigate, respond and take corrective actions to address queries or complaints.

## PROCEDURE

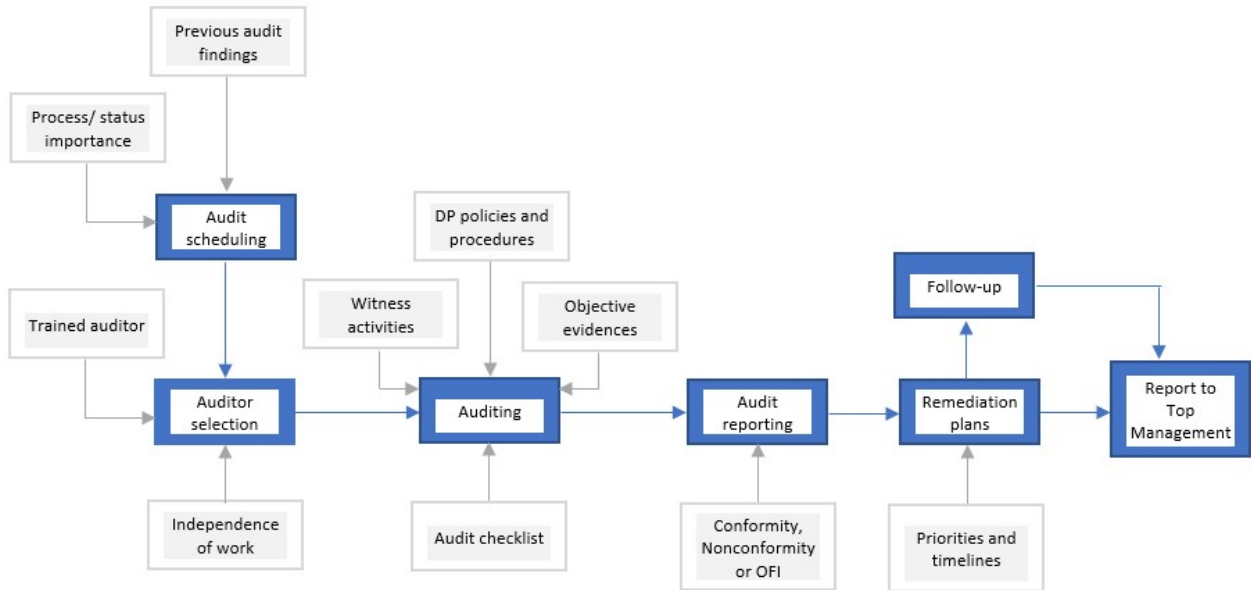
### 1. MONITORING OF COMPLIANCE WITH POLICIES & PRACTICES

- 1.1 Employees / contract staff will be required to acknowledge applicable policies on data protection and information security through the DPMP-PRO-11-F6 Acknowledgment of Policies and Rules.
- 1.2 The DPO shall conduct compliance checks on a quarterly basis to monitor compliance with data protection policies and uncover blind spots using the DPMP-PRO-11-F1 Quarterly Compliance Inspection Checklist. The results shall be submitted to the The Management for acknowledgment on the checklist, and summary of findings or issues to highlight shall be shared to all employees by the DPO for necessary action and to serve as reminders on handling personal data responsibly. The communication shall be recorded using DPMP-PRO-11-F7 Acknowledgment of Policies and Rules Management.
- 1.3 Designated internal auditors shall conduct an Internal Audit on the DPMP at least once a year.

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	5 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

- The DPO works with the assigned auditor to prepare the DPMP-PRO-11-F2 Internal Audit Schedule.
- The schedule includes all processes, services and systems of the organization that involve the handling of personal data, and is based on the status and importance of the area being audited.
- Other considerations include the results of previous audits and changes impacting the organization.
- The schedule identifies when the audits will take place and what areas to be audited:
  - Each process, service or system is audited a minimum of 1 time per year.
  - The DPO assigns internal auditor(s) independent of the process, service or system to be audited.
  - The assigned internal auditor(s) should have basic knowledge and skills in complying with the PDPA (e.g., Fundamentals of the PDPA training certificate or other relevant data protection certificates).
  - The assigned internal auditor confirms the audit schedule with the assigned auditee(s).
- The assigned auditor performs the internal audit according to the DPMP-PRO-11-F3 Internal Audit Checklist.
- Auditors document the audit findings on the DPMP-PRO-11-F4 Internal Audit Report.
- The assigned auditor discusses the audit findings to the process owner. The process owner shall respond within 1 week to the auditor to agree on actions / remediation plans and target date for closure.
- The identified actions / remediation plans shall be implemented by the process owner as agreed with the auditor.
- As a guide, any nonconformities shall be prioritized and addressed from immediate to 1 month, and OFIs may be addressed within 3 months. If longer time will be required, the extended timeline must be approved by the Top Management.
- The assigned auditor verifies the actions taken on the agreed target date to ensure that identified gaps have been addressed effectively.
- The DPO shall compile the outcome of the internal audit which shall include the gaps identified (NC or OFI) and the actions / remediation plans to improve DP compliance and report status to Top Management.

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	6 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0



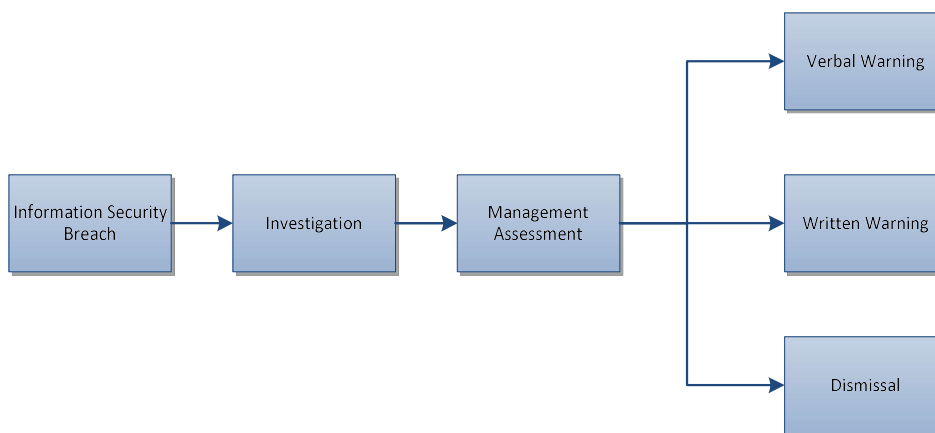
*Flow 2: Internal Audit Process*

- 1.4 The organization shall document outcomes of all reviews and conduct a management meeting at least once a year to report the outcomes to the top management. The meeting shall be recorded in DPMP-PRO-11-F5 Management Report.
- 1.5 Significant outputs from the meeting, relevant actions, and changes as a result of decisions taken during the management review shall be communicated to relevant employees.
- 1.6 Policies and procedures with respect to personal data lifecycle from collection, use and/or disclosure to disposal and the data inventory map (DIM) will be reviewed at least once a year and as and when there is any change in processes, systems, services, emerging technologies, significant feedback from stakeholders, or any changes in legal, regulatory requirements, relevant sectoral and international guidelines to ensure suitability, adequacy and relevancy.

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	7 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

## 2. VIOLATION HANDLING

- 2.1 An employee found to have violated the organization’s data protection policies and practices may be subject to disciplinary action, up to and including termination of employment.



- 2.2 The process is initiated by the detection of an information security breach. This may be a relatively minor event such as the unauthorized use of someone else’s user account or something more major such as the deliberate theft of confidential information. The handling of the breach itself will be according to the procedures set out in the DPMP-PRO-03 Data Breach Management.

### 2.3 Investigation

At an appropriate time after the information security breach has occurred, an investigation will be carried out by an appropriately trained and experienced person to establish:

- The circumstances of the breach, including date, time, sequence of events, information and systems affected.
- The root cause of the breach.
- The immediate effect of the breach on the organization.
- Whether existing policies and procedures were followed.
- If not, then whether the breach would have been avoided if existing policies and procedures had been followed.
- The individuals involved.

The results and conclusions of the investigation will be documented.

### 2.4 Management Assessment

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	8 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

In the event that the investigation concludes that there may be a case for disciplinary action against one or more individuals, an assessment will be carried out to be facilitated by HR to decide on the next steps. The person involved in this assessment should include:

- The employee's immediate superior
- HR
- The DPO
- The Management

The individual employee may be requested to participate in parts of the assessment if appropriate. Minutes of the assessment meeting(s) will be taken. In some circumstances it may be appropriate to suspend the employee whilst the management assessment is taking place.

The outcome of the management assessment will be a decision regarding which of the following actions to take:

- No disciplinary action
- Verbal warning
- Written warning
- Dismissal

The action should be communicated to the employee by the employee's manager / head of department.

## 2.5 No Disciplinary Action

If the breach is not felt to warrant disciplinary action based on investigation, then other steps may be taken to prevent a recurrence such as informal advice, training, coaching and counselling. This will not be recorded on the employee's file.

## 2.6 Verbal Warning

If there is sufficient cause for formal disciplinary action but the circumstances are relatively minor and/or it is the first time it has happened, then a verbal warning may be given.

A note of this warning will be placed on the employee's file but will be disregarded after 12 months from the date of the warning.

The action should be communicated to the employee by the employee's manager / head of department. The employee has the right to appeal against a verbal warning.

## 2.7 Written Warning



<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	9 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

For more serious breaches or repeated breaches for which a verbal warning has previously been issued, a written warning may be given. This will specify the reason for the warning, the improvement that is required and will specify a timeframe for that improvement. A review should be held at the end of that timeframe to assess whether the required improvement has happened. If it has not, then further disciplinary action such as a final written warning or dismissal may result.

The written warning will be placed on the employee's file but will be disregarded after 2 years from the date of the warning.

The action should be communicated to the employee by the employee's manager / head of department. The employee has the right to appeal against a verbal warning.

## 2.7 Dismissal

In the case of a grave single breach or repeated breaches for which warnings have previously been issued, it may be decided that dismissal is likely to be the most appropriate action. This may also be the case if it is judged that behaviour amounting to gross misconduct has occurred.

In these circumstances, the case against the employee should be set out in writing and copies of any relevant evidence provided to the individual concerned. A formal hearing will then be held to give the employee an opportunity to respond.

After the hearing, the employee's manager / head of department will inform the employee of the final decision which will also be provided in writing. The employee has the right to appeal against dismissal.

## 2.8 Appeal

In the event that the employee wishes to exercise a right to appeal this must be notified in writing to HR within two weeks of the disciplinary decision.

An appeal hearing will be held which will be chaired by The Management, and where required a legal representative. The result of the appeal will be communicated to the employee in writing. No further appeals will be permitted.

<b>THE SOFTWARE PRACTICE PTE LTD</b>	No of Pages	10 of 10
	Document Classification:	Internal
	Effective Date	10 June 2024
<b>COMPLIANCE MONITORING &amp; VIOLATION HANDLING</b>	Doc No	DPMP-PRO-11
	Revision	1.0

**FORMS**

DPMP-PRO-11-F1	Quarterly Compliance Inspection Checklist
DPMP-PRO-11-F2	Internal Audit Schedule
DPMP-PRO-11-F3	Internal Audit Checklist
DPMP-PRO-11-F4	Internal Audit Report
DPMP-PRO-11-F5	Management Report
DPMP-PRO-11-F6	Acknowledgment of Policies and Rules
DPMP-PRO-11-F7	Acknowledgment of Policies and Rules Management