

Data Protection Procedure

Effective Date: 05.09.2025

Revision: 1

Company: HAWK FILTRATION (SEA) SDN BHD (SEA) SDN. BHD.

Location: Malaysia

1. Purpose

To establish a structured framework for the collection, processing, storage, use, and disclosure of personal data at Hawk Filtration (SEA) Sdn Bhd, ensuring compliance with the Personal Data Protection Act 2010 (PDPA), Workplace Conditions Assessment (WCA) standards, and internal ethical commitments.

2.0 Definitions

Term	Definition
Personal Data	Information relating to an identifiable individual processed as part of a commercial transaction.
Sensitive Personal Data	Data related to health, beliefs, political opinions, criminal records, or other sensitive categories under PDPA.
Data Subject	The individual to whom personal data relates.
Data User	A person who processes or controls the processing of personal data.
Processing	Any operation performed on personal data, including collection, use, disclosure, storage, or destruction.
Privacy Incident	Any unauthorized access, use, disclosure, loss, or breach of personal data.

3.0 Scope

This procedure applies to all employees (permanent, contract, temporary), directors, and third-party contractors or suppliers who access or handle personal data in any form at Hawk Filtration (SEA) Sdn Bhd.

4.0 Roles and Responsibilities

Role	Responsibilities
Management	<ul style="list-style-type: none">- Oversee privacy governance structure- Approve policies and resources- Ensure third-party contracts include privacy clauses
Human Resources (HR) Department	<ul style="list-style-type: none">- Manage employee data lifecycle- Coordinate onboarding/offboarding- Lead incident response and reporting
Designated IT Personnel	<ul style="list-style-type: none">- Implement technical safeguards- Monitor systems for breaches- Support forensic analysis during incidents
Employees	<ul style="list-style-type: none">- Follow data protection policies- Report suspected breaches- Maintain confidentiality and password hygiene
Third-Party Processors	<ul style="list-style-type: none">- Comply with contractual privacy clauses- Notify Hawk Filtration (SEA) Sdn Bhd of any breach- Cooperate in audits and assessments

5.0 Procedure

5.1 Data Protection Principles (PDPA Aligned)

5.1.1 General Principle

- Data is collected only as needed.
- Must be adequate, relevant, limited to what is necessary, and not excessive.
- Used only for intended purposes with consent.
- Explicit consent is required for sensitive data.
- Data minimization applies at all stages.
- Data subjects may withdraw consent unless legally restricted.
- Protected from misuse and loss from unauthorised access, modification, or disclosure.

5.1.2 Notice and Choice Principle

- The purpose of data collection is communicated.
- Procedure and policy are available upon request.

- Notice must be provided in English and Bahasa Malaysia.

5.1.3 Disclosure Principle

- Disclosure only to authorized internal/external parties.
- Includes insurers, medical providers, clients, and contractors.
- Data may be shared with clients assessing Hawk Filtration (SEA) Sdn Bhd's capabilities.

5.1.4 Security Principle

- Strong safeguards applied.
- Access to data restricted by passwords.
- IT communication between office computer devices and the internal/external network is firewall-protected.
- Printed sensitive data shall be marked “confidential”.
- Laptops must be kept secure and encrypted.
- Sensitive data and documents should be saved using confidential passwords.
- Server data is replicated and backed up across secure storage.
- Disaster and continuity plans are activated when necessary.

5.1.5 Retention Principle

- Data is retained only as long as necessary.
- Former employee data retained for legal or HR purposes.

5.1.6 Data Integrity Principle

- Data is accurate and updated.
- Employees must notify HR of any personal information changes promptly. These include changes to the following: -
 - Name;
 - Home address;
 - Contact telephone numbers;
 - Next of kin;
 - Dependents (e.g., for private medical insurance purposes, if applicable);

- Beneficiaries (e.g., for death in service benefit, if applicable);
- Persons to be notified in case of emergency;
- Bank details for salary payment; and
- Tax File Number (if applicable)

5.1.7 Access Principle

- Data subjects may access and correct their data.
- The information held by Hawk Filtration (SEA) Sdn Bhd about an employee will be made available to the employee on request, together with a description of the purposes for which Hawk Filtration (SEA) Sdn Bhd keeps this information and to whom it may be disclosed.
- Anonymous access is possible where lawful.

5.2 IT Hardware and Software Usage

5.2.1 Software Usage

- Only authorized software is allowed.
- Employees must not install or copy software without approval.
- Report suspected viruses and malware to IT immediately.

5.2.2 Internet and Intranet Usage

- For work and professional use.
- No access to inappropriate content.
- No personal profit, unlawful, or political use.
- Confidential info not to be emailed to unauthorized recipients.

5.2.3 Email Usage

- Email is a business communication tool. Users are obliged to use this tool in a responsible, effective, and lawful manner.
- The Hawk Filtration (SEA) Sdn Bhd email is for business use.
- Passwords must be private and updated regularly.
- Sensitive emails must be Director-approved and encrypted.
- Good practices in subject lines, privacy, and replies are required.

- Forwarding of chain letters, junk mail, jokes, and executable files is strictly forbidden.
- Do not send mass mailings.

5.2.4 Data Transmission & Monitoring

- Hawk Filtration (SEA) Sdn Bhd monitors internet, emails, IMs, and file transfers.
- May block access to certain content, such as pornography and gaming. Should an employee access a prohibited website, then it will be deemed as gross misconduct and could result in disciplinary action.
- Random inspections of hardware by IT are permitted.
- VPN or proxy use is prohibited unless approved.
- If an employee has to send confidential information and data by email, the following guidelines must be adhered to: -
- Must secure the information by converting the attachment document into a PDF and adding password protection. The employee shall send the attachment and inform the recipients that the password will be sent to them via a separate email.
- Before sending the password, the employee shall verify all recipients' email addresses to ensure that there is no mistaken delivery to the wrong addressee.

5.3 Legal Risks and Compliance

5.3.1 Email/internet misuse can result in legal or disciplinary action.

5.3.2 Hawk Filtration (SEA) Sdn Bhd dissociates from unlawful user conduct and will investigate privacy-related misconduct.

5.3.3 It is important that employees are aware of the legal risks of sending and receiving email: -

- If an employee sends and/or forwards emails that contain any libelous, defamatory, offensive, racist, or obscene remarks, the employee and Hawk Filtration (SEA) Sdn Bhd can be held liable.
- If an employee unlawfully forwards confidential information, the employee and Hawk Filtration (SEA) Sdn Bhd can be held liable.
- If an employee unlawfully forwards or copies messages without permission, the employee and Hawk Filtration (SEA) Sdn Bhd can be held liable for copyright infringement.

- If an employee sends an attachment that contains a virus or malware, the employee and Hawk Filtration (SEA) Sdn Bhd can be held liable.
- Breaches involving PII will be escalated to the designated SC-MR.
- Legal counsel may be consulted for serious violations involving data misuse or unauthorized disclosure.
- Complaints and misconduct are to be handled as per the internal “Managing Misconduct, Disciplinary and Grievance” Procedure.

5.4 Privacy Incident Management Procedure

In the case of any privacy incidents occurring, Hawk Filtration (SEA) Sdn Bhd shall follow the structured privacy incident management process:

5.4.1 Identification

- Any employee who suspects a privacy breach (e.g., unauthorized access, disclosure, loss, or misuse of PII) must report it immediately to HR or IT.
- Incidents may be detected via system alerts, employee reports, audits, or third-party notifications.

5.4.2 Containment

- IT will isolate affected systems or devices to prevent further exposure.
- HR will notify impacted individuals and initiate internal documentation.

5.4.3 Assessment

- A cross-functional team (HR, IT, Management) will assess the scope, type of data involved, and potential impact.
- Determine whether external reporting (e.g., PDPA authority or clients) is required.

5.4.4 Notification

- Affected individuals will be informed of the breach, its nature, and recommended actions.
- External authorities will be notified if required by law or contractual obligations.

5.4.5 Remediation

- The cross-functional team will implement corrective actions (e.g., password resets, access revocation, system patching).
- Review and update policies or controls to prevent recurrence.

5.4.6 Documentation

- All incidents will be logged in the Privacy Incident Register.

- Records will include date, nature, parties involved, actions taken, and closure status.
- Retained for a minimum of 5 years for audit and review.

5.5 Privacy Contractual Clauses with Subcontractors & Suppliers

- All subcontractors processing PII must sign a Data Protection Agreement (DPA) or Non-Disclosure Agreement (NDA) that includes privacy clauses in service contracts.
- Clauses must cover confidentiality, data handling, breach notification, and compliance with PDPA and WCA standards.
- Hawk Filtration (SEA) Sdn Bhd reserves the right to audit subcontractor practices and terminate contracts for non-compliance.

5.6 Breach Notification

5.6.1 Breaches must be reported to authorities and affected parties if required by law.

6. Review and Updates

- This procedure is reviewed annually or as needed due to regulatory or business changes.
- Updates must be approved by management and communicated to all concerned employees.

7. Reference

- Personal Data Protection Act 2010 (Malaysia)
- WCA & SMETA Standards

Approved by:

Cyndi Lim | Management Representative – Labor & Business Ethics

Date: 05.09.2025