Public Packages Holdings Berhad
Information Security Policy

Introduction

Public Packages Holdings Bhd ("PPHB") and its subsidiaries (collectively referred to as "The Group") are committed to maintaining resilient, secure and trusted digital environment. Cybersecurity is embedded into governance, operations, and risk management framework to safeguard the confidentiality, integrity, and availability of information assets across the Group.

This Information Security Policy ("Policy") is prepared in accordance with the Cyber Security Act 2024, the Personal Data Protection Act ("PDPA") 2010 and Bursa Malaysia Cyber Risk Management Guidelines. It outlines the principles, responsibilities, and controls required to protect PPHB's information assets across all business activities.

This Policy complements and should be read in conjunction with, the Group's Code of Conduct and Ethics and Personal Data Protection Policy, available at **www.pph.com.my**.

Purpose

The purpose of this policy is to: -

(a) Establish a unified and structured information security framework;
(b) Prevent unauthorised access, disclosure, alteration, or destruction of information assets;
(c) Ensure business continuity and regulatory compliance; and
(d) Promote strong cybersecurity practices across the organisation.

This policy applies to all employees, contractors, consultants, suppliers, customers and business partners who access PPHB's information or systems. All personnel are accountable for complying with this Policy.

Scope

This policy covers all information, in any format (digital, physical and verbal), that is created, processed, transmitted, stored and disposed of by PPHB.

It applies to: -

a) **Hardware**
All physical assets used to process and store information, computers, servers, networking equipment, and communication devices.

b) **Software**
All applications and systems used within the Group, including operating systems, application software, database management systems, networking software, and productivity tools.

c) **Data or Information**
All factual content, whether in paper or electronic forms, that supports the Group's mission and operations. This includes documentation systems, procedures, records, employee and customer data, databases and archived files.

d) **Personnel and external parties**
All individuals with tasks or responsibilities supporting Group's mission, including employees and authorised third parties.

e) **ICT facilities including server rooms**
Physical locations used to store and manage ICT assets, such as server rooms, data centres and communication hubs.

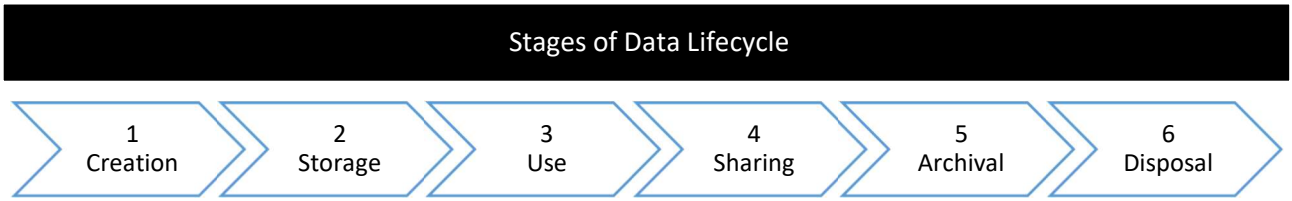
f) **Communication and network infrastructure**
PPHB safeguard all ICT assets to ensure secure, accurate, reliable, and timely access in support of operational and stakeholder requirements.

Governance

PPHB adopts a top-down approach to information security to ensure that security controls are practical, effective, and consistently applied across the Group.

The Compliance Team, led by the Group Management Director and Data Protection Officer ("DPO"), is responsible for identifying and accessing potential risks through a structured ***risk management and treatment process***, and ensuring the effectiveness of implemented controls. Details are outlined under **Appendix C**.

Data Lifecycle Management



The Group enforces a six-stage **data lifecycle model** to ensure consistent protection from creation to destruction. This lifecycle forms the foundation of all solution design, development, implementation and operations activities, ensuring that data, whether digital and physical, is safeguarded against internal and external threats.

Key focus areas aligned with the data lifecycle are detailed in **Appendix B**.

Data Security Measures

1. **Data Handling and security**

Data Handling

All information stored in PPHB's systems is the property of the Group. Data must: -

(a) Be classified appropriately;
(b) Be accessed strictly on business needs only;
(c) Be encrypted when sensitive or high-risk;
(d) Not be stored on unauthorised devices or systems.

Users must exercise sound judgement when handling data. Confidential information must not be sent, uploaded, transferred to portable media or non-PPHB systems unless explicitly authorised as part of official duties.

In addition, employee must: -

a. Avoid transferring sensitive data (e.g. customer information, employee records, and etc) to personal devices;
b. Share confidential data only through approved and secured channels; and
c. Report cybersecurity threats (e.g. phishing, malware, hacking attempts) immediately.

PPHB reserves the right to monitor systems usage and access logs, subject to applicable laws.

Malware Protection

Users must take reasonable precautions to prevent malware infections. All suspected or confirmed malware incidents must be reported to the IT department immediately.

Acceptable Use of IT Systems

Limited personal use is permitted, provided it does not:

a. Affect productivity;
b. Introduce security risk: and
c. Contravene Group policies.

Periodic IT audits will be conducted to ensure compliance.

2. Password control

Passwords must: -

a) Contain at least six (6) characters in length and combination of letters, numbers and special characters;
b) Not contain user identifiers; and
c) Be changed at least once every three (3) months.

Users are required to maintaining confidentiality of their passwords and must never share their account credentials with others.

3. Emails

Users must comply with guidelines below: -

a. Business email use must comply with all Group's policies.
b. The use of personal email account for business purpose is prohibited.
c. Emails should be retained only if they qualify as business records.
d. Offensive, disruptive or inappropriate emails are prohibited.
e. Automatic forwarding Group's email to external email systems is not allowed.

PPHB may review email content as permitted by law.

4. Backup and Recovery

Backup data should be stored at secure location separate from the primary data source. Access to backup storage areas must be locked, monitored by CCTV, and logged.

The IT department is responsible for performing and documenting weekly backups. These measures ensure the integrity, availability and recovery of critical data, enabling prompt restoration in the event of system failures or loss incidents.

Portable storage media must be clearly labelled. These devices must not be removed from the company premises without proper authorisation.

5. Network Security

PPHB's network architecture shall be designed according to security-by-design principles with controls including firewalls, intrusion detection and prevention systems (IDS/IPS), secure virtual private networks (VPN), and network segmentation.
Network configurations must: -

a. follow approved standards;
b. be reviewed annually or upon major infrastructure changes; and
c. be logged and reviewed through the change-management process.

Remote access is restricted to authorized personnel using **encrypted channels and session timeout mechanism.**

6. Third party Security (Vendors and Outsourcers)

All vendors must sign confidentiality and data-processing agreements before accessing any company information or systems.

The IT and Compliance teams shall perform due diligence and perform risk assessments on all service providers to before granting access.

Third-party source code must be securely managed, reviewed, tested, and stored in secure repositories under PPHB's control.

PPHB may suspend or terminate vendors relationships in case of non-compliance.

7. Mobile Devices Security

The Company requires all mobile devices used to access corporate information — including laptops, smartphones, and tablets — to be registered with the IT Department.

Since the Company does not operate a Mobile Device Management (MDM) system, device compliance is managed through manual recording, periodic checks, and user declarations.

Devices must be encrypted, password-protected and auto-locked after periods of inactivity. The installation of unauthorized applications and the use of unsecured Wi-Fi networks are prohibited.

Lost or stolen devices must be reported immediately to the IT Department for initiate data-wipe procedures. Bring-Your-Own-Devices ("BYOD") usage is allowed only with written approval.

Cyber Security Training Awareness

PPHB recognises the importance of cybersecurity awareness. While formal programs are being developed, basic security practices are communicated during onboarding and through internal communications. The Group is committed to progressively enhancing cybersecurity training.

Incident Management

All incidents must be reported within two (2) hours of detection, while initial NC4S report must be reported within six (6) hours, followed by a supplementary report within fourteen (14) days.

Incident response activities will follow the phases below: -

Phase	Description	Sample Actions
Identification	Detect and classify the incident	Alerts, reports, anomaly detection
Containment	Limit or prevent further spread	System isolation, account disablement
Eradication	Remove the threat from the environment	Malware removal, patching
Recovery	Restore and resume normal operations	Backup restoration, enhanced monitoring
Notification	Inform relevant stakeholders	Regulatory notifications, internal and external communications
Review	Regulatory notifications, internal and external communications	Root cause analysis, policy and playbook updates

Documentation, evidence preservation, and post-incident reviews are mandatory. Findings from incidents will be used to update playbooks, controls, and training materials. Continuous improvement is supported through quarterly simulations, audits and awareness activities support continuous improvement.

Organisational Roles and Responsibilities

Role	Key Responsibilities
Board and Executive	Endorse policy, allocate resources, and provide overall risk governance.
DPO	Lead compliance initiatives, manage incident reporting, and oversee data governance.
Information Security Officer ("ISO")	Maintain the ISMS, manage risks, and update security policies.
IT & Cybersecurity Team	Technical controls, monitoring, investigations
Data/System Owners	Define data classification, approve system access, and ensure secure configuration.
Department Heads	Enforce compliance within their teams and ensure staff training.
Legal & HR	Advise on regulatory communication requirements and any necessary disciplinary actions.
All Personnel	Protect information assets, follow security policies, and report incidents promptly.

Audit and Compliance

Type	Description	Frequency
Internal	Conducted by internal personnel	Periodically or as needed
External	Conducted by third parties or certification bodies	Annually or under certification
Regulatory	Conducted by government authorities	As mandated
Technical	Review of systems, configurations, and access controls	Quarterly or as needed
Operational Technology ("OT")/ Industrial Control Systems ("ICS")	Assessment of manufacturing systems and network segmentation	On request

Audit findings must be remediated within agreed timelines and records retained for a minimum of three (3) years.

Review and Continuous Improvement

This Policy will be reviewed annually or updated to reflect in laws and regulations.

Appendix A
Group's key areas of information security

1. **Organisation for information security**	• What are your roles and respnsibilities as a **Data Owner**, **System Owner and Data User** to ensure information is secured?
2. Information Classification	• What are **the information classfication categories,** and how you should: • Classify a **document containing multiple types classified information?** • Handle **change in information classification?** • **Classify information received from third parties?** • **Review** and **update** information classification regularly.
3. Information labeling and handling	• How should you lable and handle **documents**, **information media**, **printing**, **storage**, **filing**, **backup**, **retention** and **disposal**? • What the best practices to protecting information while working in the **office or home**.
4. Access control	• How you can ensure secure access control when accessing **filing rooms**, **IT systems** and **end-user computing devices**?
5. Information sharing	• What security measures should you should take when sharing information: • internally and externally? • using messaging applications? • on social media?

Appendix B

Data Lifecycle Controls

Stage	Definition	Required Security Control	Roles
1 Creation	Data is created, acquired, or received into PPHB systems	• Classify data immediately (Public / Internal / Confidential / Restricted) • Store only on authorised and backed-up systems	Data Owners System Owners
2 Storage	Data is retained and maintained for operational use	• Encryption of Confidential & Restricted data • Access control (least privilege) • Version control and metadata accuracy	IT System Owners
3 Use	Data is accessed, processed, or shared in daily operations	• Authorised use only • Secure communication channels • MFA for privileged access • Activity logging and monitoring	All Personnel
4 Sharing / Transfer	Data is circulated internally/externally	• Data Sharing Approval required • NDA and contractual controls for vendors • Encryption during transfer • Prohibit use of personal email/systems	Data Owners
5 Archival	Data retained for legal, regulatory, or operational history	• Defined retention periods • Secure and controlled storage • Annual review for relevance	Data Owners DPO
6 Disposal	Data is destroyed when no longer required	• Secure destruction methods (shredding, DLP secure erase) • Disposal authorisation required • Maintain destruction records	IT System Owners

Data Classification (Mandatory)

Classification	Description	Examples	Protection Required
Restricted	Highly sensitive. Unauthorised exposure causes major damage.	Legal, payroll, personal data, cybersecurity records.	Strong encryption, strict access control.
Confidential	Sensitive internal content.	Financial data, internal reports, system configs.	Controlled access, approved sharing only.
Internal	Used for normal operations and low harm if disclosed.	Procedures, templates.	Standard security controls.
Public	Approved for public distribution.	Corporate website content	No confidentiality controls

*** Retention periods must comply with regulatory and contractual requirements.*

*** Exceptions require DPO approval.*

Appendix C
Cyber Risk Management & Treatment Framework

PPHB follows a structured risk management approach aligned with national cybersecurity mandates and Bursa Malaysia's guidelines.

1 Risk Identification

Sources include:
- Threat intelligence
- Vulnerability assessments and pretests
- IT monitoring alerts
- Incident reports
- Vendor risk assessments
- Regulatory requirements

2 Risk Evaluation and Categorisation

Risks are evaluated using:
- Likelihood (how probable the event)
- Impact (damage to confidentiality, integrity, availability)

Risk scoring determines:
- High priority — Immediate mitigation required
- Medium priority — Management-approved timeline
- Low priority — Acceptable with monitoring

3 Risk Mitigation

Treatment Type	Description	Examples
Avoid	Stop risky activity.	Remove unsupported system
Mitigate	Apply control to reduce risk	Firewall, encryption
Transfer	Share risk with 3rd party	Cyber insurance, outsourcing
Accept	Approved residual risk formally	Low-impact systems

All high-risk items must have a remediation plan with deadlines.

4 Risk Monitoring & Review

- Quarterly cybersecurity risk reporting to Management
- Annual review of risk posture
- Continuous monitoring of critical systems
- Vendor compliance tracked via scorecards

Changes in the environment (technology, threats, regulation) trigger reassessment.

5 Documentation Requirements

The following must be recorded and retained:
- Risk register
- Treatment plans
- Evidence of control implementation
- Periodic review results
- Incident and audit findings

DPO is responsible for maintaining this documentation.