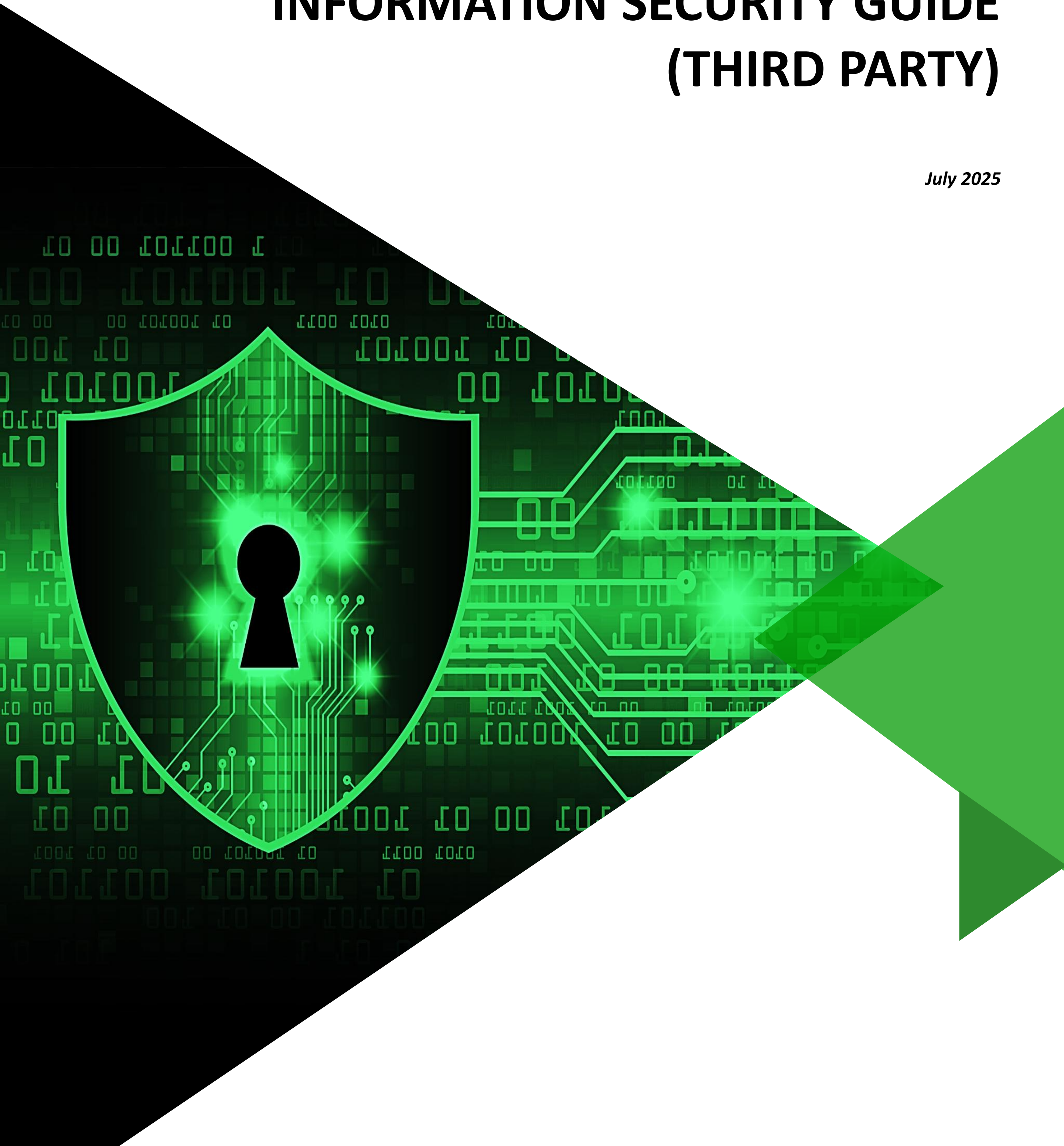
A member of UEM

PLUS MALAYSIA BERHAD

INFORMATION SECURITY GUIDE (THIRD PARTY)

July 2025



CONTENT

TERMINOLOGY, ABBREVIATIONS & DEFINITION

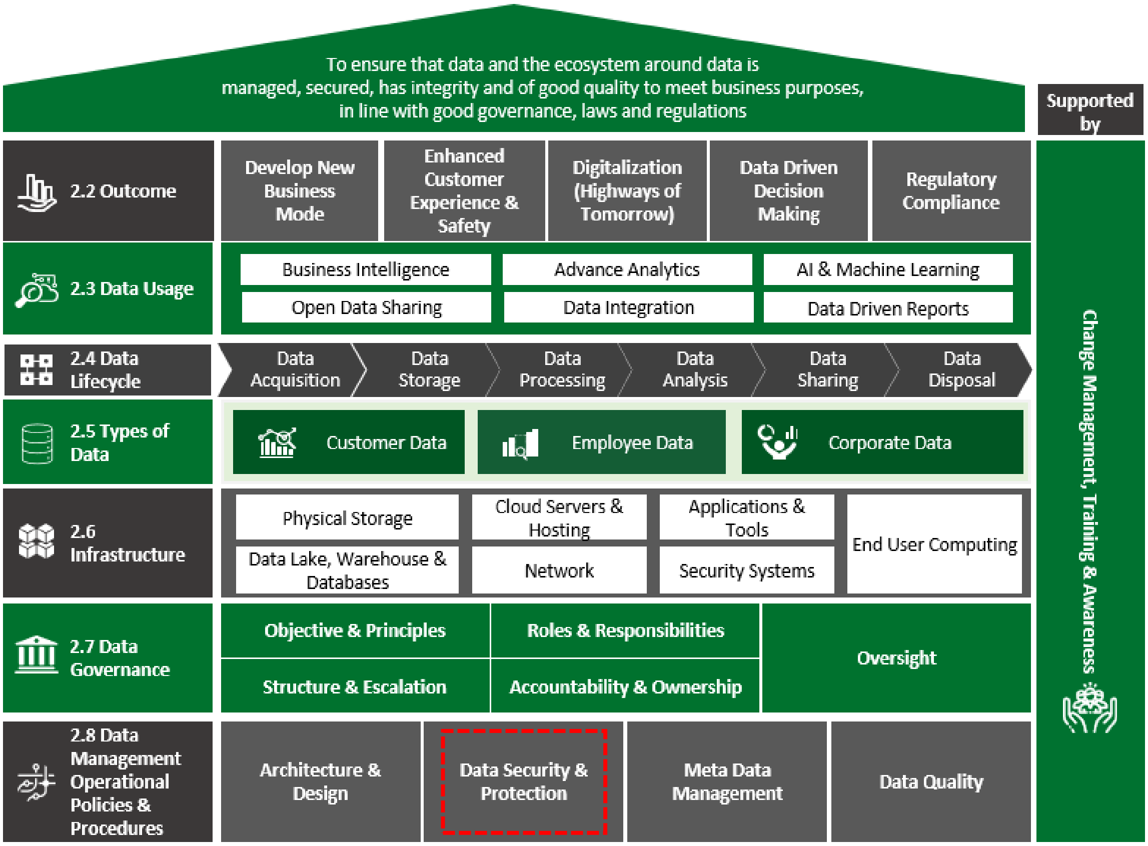
For the purpose of this Information Security Guide (Third Party) ("IS Guide"), the terms used are defined as follows:

No.	TERMINOLOGY/ ABBREVIATIONS	DEFINITION
1.	AI	refers to artificial intelligence.
2.	Authorised Third Party	refers to PMB's contractors, agents, third-party suppliers or service providers with whom PMB enters into an agreement.
3.	C&I	refers to Compliance & Integrity Function.
4.	Information medium	refers to storage devices (e.g. electronic files stored in servers, notebooks, thumb drives, hard drives, CD, film/ video tapes, memory cards, camcorders, cameras micro films, Universal Serial Bus ("USB") drives, hard drives, DVDs, diskettes and Blu-ray Disc) and physical infrastructure (e.g. physical storage, data lake, warehouse, database, cloud servers and hosting, network, applications and tools, and end-user computing such as laptops, desktop computers, printers and mobile phones).
5.	IS Guide	refers to this Information Security Guide (Third Party), unless stated otherwise.
6.	PMB	refers to PLUS Malaysia Berhad and its Group of Companies (collectively hereinafter referred to as "PMB", "we", "us" or "our").
7.	PMB personnel	refers to any person who has entered into an employment contract with PMB, including permanent and contract employees, any person who is a temporary employee or under any internship programme and members of PMB Board of Director (including executive and non-executive).
8.	Social media	refers to online blogs, forums, messaging sites and social media websites including but not limited to Facebook, Twitter, Instagram, TikTok, LinkedIn, YouTube, etc.
9.	Third Party	refers to PMB's business associates (i.e. PMB's business associates, which includes business partners, vendors, contractors, sub-contractors, consultants, agents, representatives, tenants and other intermediaries who are performing work or services, for and on behalf of PMB), all parties engaging with PMB or have intention to engage with PMB in the future and other parties requesting for PMB's information (hereinafter referred to as "you" or "your").
10.	Messaging application	refers to an application that allows users to send and receive information instantly such as WhatsApp, Telegram, WeChat, Line, Google Hangouts, Facebook Messenger, Viber etc.

PMB'S POSITION ON INFORMATION SECURITY

DATA GOVERNANCE FRAMEWORK

In line with PLUS Malaysia Berhad's ("PMB") Data Governance Framework which sets the overarching guiding principles and methodology for managing enterprise data across PMB holistically throughout the six (6) stages of data lifecycle, one of the key priority areas is on "**data security and protection**" as highlighted in the red box below:



To ensure that data and the ecosystem around data is managed, secured, has integrity and of good quality to meet business purposes, in line with good governance, laws and regulations

Supported by

2.2 Outcome	Develop New Business Mode	Enhanced Customer Experience & Safety	Digitalization (Highways of Tomorrow)	Data Driven Decision Making	Regulatory Compliance	Change Management, Training & Awareness
2.3 Data Usage	Business Intelligence Open Data Sharing	Advance Analytics Data Integration	AI & Machine Learning Data Driven Reports			
2.4 Data Lifecycle	Data Acquisition	Data Storage	Data Processing	Data Analysis	Data Sharing	Data Disposal
2.5 Types of Data	Customer Data	Employee Data	Corporate Data			
2.6 Infrastructure	Physical Storage Data Lake, Warehouse & Databases	Cloud Servers & Hosting Network	Applications & Tools Security Systems	End User Computing		
2.7 Data Governance	Objective & Principles Structure & Escalation	Roles & Responsibilities Accountability & Ownership	Oversight			
2.8 Data Management Operational Policies & Procedures	Architecture & Design	Data Security & Protection	Meta Data Management	Data Quality		

Table 1: Data Governance Framework

To ensure that the governance of data security and protection for PMB's information and other third party's information provided to PMB are at the highest level, PMB has set the following **key principles** on data security and protection:

1. Maintain effective control and classification over data privacy to preserve the confidentiality and integrity of data throughout its lifecycle; and

2. Ensure all data, both digital and physical are secured and protected against internal and external threats.

To achieve the above-mentioned principles, PMB has developed this Information Security Guide (Third Party) ("IS Guide") to provide guidance for you in ensuring the security of PMB's information.

PMB’S POSITION ON INFORMATION SECURITY

OBJECTIVE

This IS Guide is targeted to achieve the following objectives:

1. Setting PMB’s expectation to ensure PMB’s information shared is adequately secured and protected by you; and

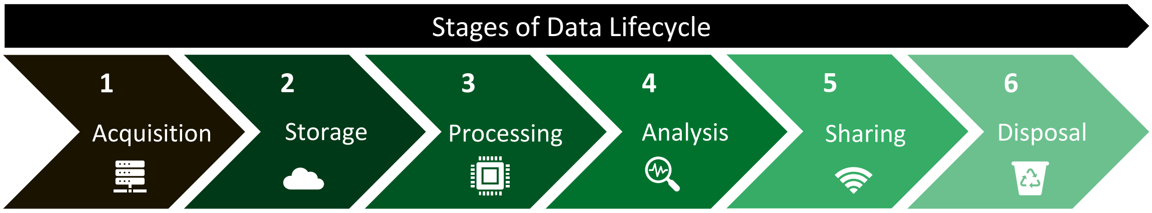
2. Providing confidence to you that PMB has implemented adequate mechanism and controls to ensure your information provided to PMB is secured and protected against internal and external treats.

PROTECTING PMB’S INFORMATION

To protect the security, confidentiality and integrity of PMB’s information, PMB has developed this IS Guide to highlight the key PMB’s information security requirement which are relevant to you as third parties in line with Malaysian laws and regulations.

The purpose of this IS Guide is to ensure that PMB’s information shared with you are adequately protected. It will provide you with a guideline to protect the security of PMB’s information, both in hardcopy and digital form, by detailing the requirement of information security controls and real life examples. Hence, this IS Guide provides PMB’s expectation on you to implement the necessary technology and cybersecurity controls.

The controls provided under this IS Guide are necessary in ensuring information security through out the six (6) stages of data lifecycle as follows:



Additionally, if you are acting as a “data processor” i.e. you are processing any personal data on behalf of PMB, you are required under Section 5 of the PDPA to comply with the Security Principle (Section 9 of the PDPA).

PROTECTING INFORMATION PROVIDED TO PMB

PMB is committed in securing and protecting any information shared with us by implementing necessary information security controls and mechanism and adhering to the requirements under PMB’s policies and procedures. This is to ensure that your information, both in hardcopy and digital form are protected against any unauthorised access, usage, disclosure, disruption, modification and destruction to preserve the confidentiality and integrity of your information.

FURTHER AMENDMENTS AND CONFLICT

PMB reserves the right to update and/or amend this IS Guide. As such, you are expected to read this IS Guide when dealing with PMB’s information.

In the event of any conflict between this IS Guide and your obligations as well as restrictions under any Non-Disclosure Agreement or any other agreements with information confidentiality and security clauses, the latter shall prevail.

QUERIES

If you have any questions or concerns, please consult your key contact person at PMB or Compliance and Integrity (“C&I”) Business Function of PMB. Refer to last page of this IS Guide for the contact details of C&I.

WHO DOES THIS IS GUIDE APPLY TO?

PMB'S BUSINESS ASSOCIATES

- This IS Guide applies to PMB's business associates, which includes business partners, vendors, contractors, sub-contractors, consultants, agents, representatives, tenants and other intermediaries who are performing work or services, for and on behalf of PMB.
- All Personnel, regardless of their position or role, are responsible to communicate this IS Guide to their business associates.

ALL PARTIES FORMALLY ENGAGING WITH PMB

- This IS Guide applies to all parties that are currently engaged with PMB or have intentions to engage with PMB in the future.
- PMB will use its influence in good faith to require the parties to understand and implement this IS Guide.

ANY PARTY REQUESTING FOR PMB'S INFORMATION

- This IS Guide applies to all parties who requested PMB's information for any other purpose including for academic research, publications, etc. this may include Government agencies, universities, research companies etc.
- PMB Personnel will be communicating with such parties to require them to understand and implement this IS Guide.

KEY HIGHLIGHTS OF INFORMATION SECURITY GUIDE

KEY HIGHLIGHTS OF INFORMATION SECURITY GUIDE

GENERAL

This IS Guide will be focusing on 3 key areas of information security for your ease of reference and implementation as a third party.

KEY HIGHLIGHTS

To understand the purpose of each area under this IS Guide, you may refer to the following highlights:

1 Information labelling and handling

How **PMB’s information is labelled** and how you should **handle PMB’s information** including areas such as **information classification, retention, disposal, protecting information while working at the office or home** as well as **using IT devices** in a secured manner.

2 Access control

How you can ensure secured access control when accessing PMB’s physical and digital information including accessing PMB’s **hardcopy documents, PMB’s systems** as well as **protecting your user ID and password.**

3 Information sharing

What are the security measures you should take when sharing PMB’s information **internally and externally** while using various platforms including **messaging application** and **social media**.

UNDERSTANDING DATA LIFECYCLE

GENERAL

When dealing with PMB's information, it is important for you to understand the information security measures being practiced by PMB throughout the six (6) stages of data lifecycle.

STAGES OF DATA LIFECYCLE

PMB expects that our information shared with you are protected by implementing the information security mechanism at each stage of data lifecycle as follows:

Stages of Data Lifecycle		Information Security Areas
Acquisition	Creation and collection of data gathered/ captured from one or multiple sources point.	• Information labelling and handling
Storage	Recording and archiving (storing) of information (data) in a storage medium such as the computer, servers, cloud, filling room, etc. for future use.	• Information labelling and handling
Processing	Conversion of raw data into usable and desired form includes image, graph, table, vector file, audio, charts or any other desired format.	• Information labelling and handling • Access control
Analysis	Inspecting, cleansing, transforming and modelling data with the goal of discovering useful information, informing conclusions and supporting decision making.	• Information labelling and handling • Access control
Sharing	Disclosure of data with multiple users as follows: • Internal (within PMB); • External (with public, external parties, regulators and Government bodies); and • Using messaging applications and social media.	• Information labelling and handling • Information sharing
Disposal	Deleting, retiring and destroying data stored on all storage medium when data reaches its end-of-life or relevancy.	• Information labelling and handling

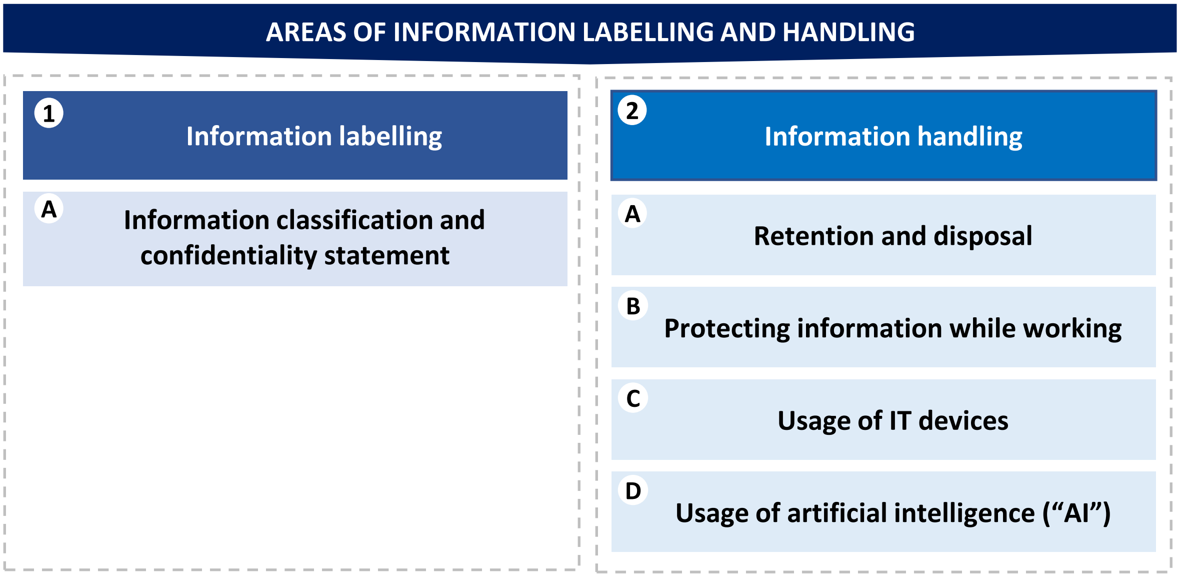
1. INFORMATION LABELLING AND HANDLING

GENERAL

There will be instances where PMB may share information with you. This may be necessary for you to fulfil your daily tasks. Therefore, it is important for you to understand what to observe when you receive information or documents from PMB and how to properly handle PMB's documents to protect its security, integrity and confidentiality.

OVERVIEW OF INFORMATION LABELLING AND HANDLING

In this section, you will be guided on how to observe the information labelling on PMB's documents and how to handle them in a secured manner. The following is the overview of the areas covered under this section:



AREAS OF INFORMATION LABELLING AND HANDLING

1 **Information labelling**

- A **Information classification and confidentiality statement**

2 **Information handling**

- A **Retention and disposal**
- B **Protecting information while working**
- C **Usage of IT devices**
- D **Usage of artificial intelligence ("AI")**

1. INFORMATION LABELLING AND HANDLING

1 INFORMATION LABELLING

A INFORMATION CLASSIFICATION AND CONFIDENTIALITY STATEMENT

GENERAL

When you receive a document from PMB, please observe the label on the document attached. It may be labelled as "Highly Confidential" or "Restricted" based on the following criteria:

Information Classification	
Highly Confidential	• Information that is provided strictly on a **need-to-know basis to you** and is considered **HIGHLY SENSITIVE.** • Not intended for sharing except with consent from PMB.
Restricted	• Information that is **restricted** to selected personnel within PMB and your company and the information **MAY BE SENSITIVE.** • Not intended for sharing except with consent from PMB.

Once you have identified the information classification, you should refer to the confidentiality statement in the same document to further understand the restriction when dealing with such information:

Confidentiality Statement

"This document is classified as **HIGHLY CONFIDENTIAL/ RESTRICTED**. Any unauthorised reproduction, disclosure, dissemination, distribution, publication and/or storage of this document is strictly prohibited. The company reserves the right to take disciplinary and/or legal action against any party responsible for such unauthorised actions."

APPLICATION

When you receive PMB's information labelled as "Highly Confidential" or "Restricted", you are only allowed to use such information in the manner agreed with PMB, i.e. strictly to perform your intended obligation or services.

Whenever necessary, PMB may also provide you with **PMB's information** that is **already publicly available**. In such situation, the **restrictions** on "Highly Confidential" and "Restricted" information **do not apply**.

For guidance on how to share PMB's information, please refer to Section 3 (Information Sharing) of this IS Guide.

CAN YOU SHARE PMB'S INFORMATION WITH OTHER PARTIES?

You are prohibited from sharing any "Highly Confidential" or "Restricted" information provided by PMB without obtaining PMB's consent. However, if you are of the view that you are obligated to share PMB's information with any parties under any agreement, laws or regulations, you should inform PMB on the matter beforehand.

For more information on how to share PMB's information, please refer to Section 3 (Information Sharing) of this IS Guide.

HOW DOES PMB CLASSIFY INFORMATION PROVIDED BY YOU?

PMB will classify and align such information according to your classification criteria, guidelines or contractual obligation, if any.

However, if you do not provide us with your criteria, guidelines or relevant contractual obligation, PMB will classify the document based on PMB's information classification.

2 INFORMATION HANDLING

A RETENTION AND DISPOSAL

To carry out your daily tasks, you may need to retain PMB's information for the duration required and/ or permitted by any relevant Malaysian laws.

If PMB's information provided to you is no longer usable or relevant, it is recommended to be disposed as follows:

Classification	Highly Confidential	Restricted
Hardcopy	Shred immediately using cross-cut shredder when no longer in use.	Shred immediately when no longer in use.
Digital	Delete and empty Recycle Bin immediately when no longer in use.	
Information Medium	Properly degauss and dispose CDs, DVDs, USB drive, dead hard drives, etc.	

B PROTECTING INFORMATION WHILE WORKING

You may be required to carry out your daily tasks whether at the office, home or any other suitable locations. Hence, it is recommended for you to undertake the following precautions to ensure that PMB's information is secured at all times:

Working from office

- ✓ When leaving workspace unattended, you should turn on **screen lock** and keep **desks** clear from displaying any "Restricted" or "Highly Confidential" documents.
- ✓ To ensure that movable IT devices are **locked** and **moved to a secure area** if left unattended.
- ✓ To **logoff and shutdown** IT devices at the end of the day.
- ✓ To avoid **discussing PMB's confidential matters** in public places.

Working away from office/ home

- ✓ To use IT devices that are equipped with **security features**.
- ✓ To keep information in any form in a **secured location**.
- ✓ To **logoff and shutdown** IT devices at the end of the day.

2 INFORMATION HANDLING

C USAGE OF IT DEVICES

GENERAL

To access PMB’s information in completing your daily tasks, you may be required to use your personal or company issued IT devices.

HOW TO PROTECT INFORMATION SECURITY WHILE USING IT DEVICES?

To ensure the security of PMB’s information, the following are the recommendations on how best to secure your IT devices while working:

Security measures for usage of IT devices

- IT devices must be secured with anti-virus. The anti-virus software must be updated whenever necessary.
- You should not use a “rooted” (Android) or “jailbreak” (iOS) IT device. This is to maintain the security of the IT device and avoid it from being compromised and vulnerable to cybersecurity attacks.
- To avoid phishing, you must avoid from accessing suspicious emails or untrustworthy websites which are aimed to steal personal information or engage in any other fraudulent activities.
- Only authorised users are allowed to connect to PMB’s infrastructure, system or application and configure its access to their IT devices.
- You should not access, monitor or use any PMB’s data, systems or networks, without authorisation.
- You should not engage in any illegal activities.
- You should always use VPN when connecting to public WiFi.

**Note: “Phishing” is a cyber crime which involves the target being contacted by email, telephone or text message by a person pretending to be representing a company, bank, institution, etc. to trick individuals in giving out their sensitive personal information such as bank details, passwords, etc. to steal data or money or to inject malware.*

2 INFORMATION HANDLING

D USAGE OF ARTIFICIAL INTELLIGENCE (“AI”)

With the technology advancement, you may be required to use artificial intelligence (“AI”) to assist your daily tasks, which include but not limited to generative AI, machine learning, natural language processing, deep learning, robotics and computer vision. Although AI may potentially expedite certain tasks, you should use it with care and guided with the following principles:

Confidentiality	• PMB’s non-public information, personal information and stakeholders’ information should not be input into AI, instead all inputs should be generic or anonymized; • Authorised Third Party (“ATP”) are required to sign Non-Disclosure Agreements; and • Ensure that all data processed by AI systems is protected from unauthorized access, disclosure, or alteration.
Compliance with laws and regulations	• The use of AI must comply with laws and regulations, which include but not limited to Personal Data Protection Act; and • You should be mindful of copyright infringement when using data or output generated from AI.
Intellectual property and ownership	• Customized algorithms, data sources, model architectures developed including the output generated for the purpose of AI are PMB’s proprietary information; and • If PMB develops custom AI models, ATP may use them only if deemed necessary by PMB. Such use must be in accordance with the licensing terms specified in their agreements, and all outputs must be produced exclusively for PMB's benefit.
Ethical use and accountability	• AI should be used ethically and responsibly; • Data and output from AI should be reviewed to ensure it is accurate, relevant, truthful and free from bias; and • Consent from PMB and relevant stakeholders should be obtained before using their data.

SCENARIOS

1.

Q In the course of completing a project with PMB, you have received information from PMB labelled as "Restricted". As this information is relevant to an article that you are writing for your personal blog, can you use this "Restricted" information for your article?

A ***No, you should not use PMB's information that you have received on your professional capacity for the purpose other than to perform your obligation or services for PMB. You should obtain PMB's approval if you intend to use such information for any personal purposes.***

2.

Q You are working with other tenants in a coworking space. If you need to print a document received from PMB, what should you do to ensure the security of PMB's information?

A ***When you are away from your workstation, you should activate screen lock on your IT devices and ensure that no confidential documents are left unattended at your workspace.***

At the best of your ability, you should use a secured printing option whereby your document can only be printed upon user authentication. If this option is unavailable, you should ensure that all your printed materials are collected from the printer immediately.

3.

Q You have printed a "Highly Confidential" PMB's document for reference. What should you do once you are done with your reference and no longer need the document?

A ***You should dispose the PMB's document printed immediately by shredding the hardcopy and removing the softcopy from your IT device, unless it is a requirement under any laws, regulations or policies to retain the document for a certain period. Upon the expiration of such period, you should dispose PMB's document accordingly.***

4.

Q Upon purchasing a secondhand mobile phone, you have discovered that it is a "jailbreak" mobile phone. As you are the appointed vendor to service a PMB's application, a mobile device is required for connection to the application to gain access. Should you use your "jailbreak" mobile phone to access?

A ***"Jailbreak" mobile phone may compromise the security of the device and render it vulnerable to information lost and other risks. Therefore, you should not use "jailbreak" mobile phone to access PMB's application.***

Kindly note that these scenarios have been designed purely for education and training purposes and do not make reference to or resemble any real incidents in the past or present

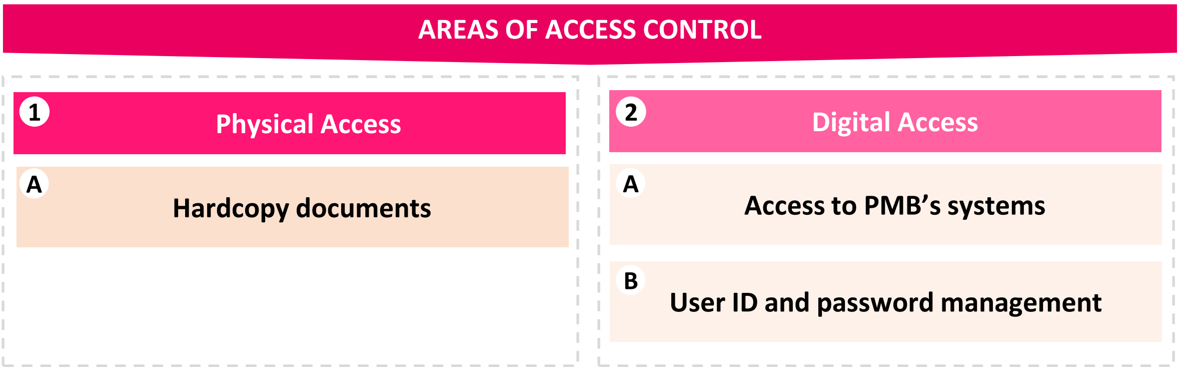
2. ACCESS CONTROL

GENERAL

To ensure that the information is properly secured and protected against cybersecurity threats, you must undertake proper security measures while dealing with PMB's information. This includes ensuring that the necessary mechanism and technology are in place to enable access control over PMB's physical and digital information.

OVERVIEW OF ACCESS CONTROL

In this section, you will be guided on your responsibilities in preventing unauthorised access to PMB's hardcopy and digital information. The following provides an overview of the areas covered under this section:



AREAS OF ACCESS CONTROL

1 Physical Access

A Hardcopy documents

2 Digital Access

A Access to PMB's systems

B User ID and password management

1 PHYSICAL ACCESS

A HARDCOPY DOCUMENTS

When receiving PMB’s hardcopy documents or printing PMB’s information, you are recommended to observe the following:

Hardcopy document

- Store PMB’s hardcopy documents in an organised, safe and secured location.
- Ensure that only authorised individuals may have access to PMB’s “Highly Confidential” or “Restricted” documents.
- If copies of PMB’s document is no longer usable or relevant, ensure that it is disposed properly. For recommendations on proper document disposal, refer to Section 1 (Information Labelling and Handling) of this IS Guide.
- PMB’s “Highly Confidential” or “Restricted” documents should not be shared with other parties who are not within your working team or your company without PMB’s consent.
- You should not leave PMB’s documents without proper filing and organisation. This may lead to document leakage and unauthorised access by other individuals.
- When printing PMB’s digital information into hardcopy, you should not leave the printed copies unretrieved from a shared printer.

2 DIGITAL ACCESS

A ACCESS TO PMB'S SYSTEMS

If your daily tasks require you to access PMB's infrastructure, systems or applications to view or retrieve relevant information, you should observe the following:

Accessing PMB's Systems	
	- You should make a formal request with business justifications to your contact person at PMB for access to the information in PMB's system. That contact person shall then obtain proper approval from PMB's management. - You may be required to execute a contract with confidentiality clause or sign a Non-Disclosure Agreement before being granted access to PMB's systems. - Upon obtaining approval from PMB's management, you will only be granted access to PMB's system limited to fulfilling your business requirements. - Upon being granted access to PMB's system, you will be provided with User ID and you will be required to set your own password. You should not share your User ID and password used to access to PMB's systems with your team members or any other parties. - You should ensure that only your authorised personnel are given access strictly on a need-to-know basis to carry out their daily tasks. - Upon completion of your contractual obligation or termination of your contract with PMB, your access to PMB's system shall be removed. - You should not attempt to access PMB's system or services without proper approval.

2 DIGITAL ACCESS

B USER ID AND PASSWORD MANAGEMENT

GENERAL

If you are granted access to PMB's system to perform your daily tasks, you will be given a User ID which then requires you to set your password. In this section, PMB will guide you on how to set, protect and manage your **User ID** and **password.**

HOW TO SET YOUR USER ID?

Upon granted access to PMB's system, you will be provided with a User ID.

HOW TO SET YOUR PASSWORD?

Upon attaining your User ID, it is important that you set a **strong password** by considering the following:

STRONG PASSWORD 👍	✓ Contains both upper and lower case characters (e.g., a-z, A-Z). ✓ Has digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|). ✓ Is at least ten alphanumeric characters long. ✓ Is not a word in any language, slang, dialect, jargon, etc. ✓ Is not based on personal information, names of family, etc.
WEAK PASSWORD 👎	× Does not meet the strong password criteria. × Same as the username. × A word found in a dictionary (English or other language). × The password is a common usage word such as: ➢ Names of family members, pets, friends, co-workers, fantasy characters, etc.; ➢ Computer terms and names, commands, sites, companies, hardware, software; ➢ Birthdays and other personal information such as addresses and phone numbers; ➢ Word or number patterns like aaabbb, qwerty, zyxwvuts, 12345678, 123321, etc.; ➢ Any of the above spelled backwards; and ➢ Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

⚠ Caution:

- If you attempt to insert the **wrong password** for 3 times consecutively, your account shall be locked and you will require Admin to manually unlock your account.
- If you do not **update password** within 75 days, your account will be automatically locked.
- If any of the above situation occurs, you should communicate with your contact person at PMB for assistance to access your account.

2 DIGITAL ACCESS

B USER ID AND PASSWORD MANAGEMENT

HOW TO MANAGE YOUR USER ID AND PASSWORD?

To access PMB's system, service or application, you must be provided with a User ID and set you own password. Hence, you are obligated to observe the following:

HOW TO PROTECT YOUR PASSWORD?

Upon setting your password, you must protect your password to avoid unauthorised access to PMB's systems, service or application by observing the following:

Managing Password and User ID

- You should change your password the latest by every 75 days. If the password is not updated within required period, your account will be automatically locked.
- You should not use any of your 15 previous passwords as your new password.
- You are prohibited from using group accounts, shared passwords or other authentication methods unless you have obtained special approval upon providing business justifications.
- You must not insert passwords into e-mail, messages or other forms of unsecured electronic communication.
- If a session is inactive for more than 30 minutes, you will be prompted for re-authentication.
- You should change your password during the first login into your account.

Protecting Password

- You should not use the same password for PMB accounts as for other non-PMB access (e.g. personal account, internet banking, internet mail and social media).
- You should not share PMB account passwords or hint about the password with anyone, including superiors, IT administrators, line management and family members either via e-mail, text message or verbally over the phone.
- You are prohibited to use shared user accounts for any PMB's system.
- You will be held responsible for all activities performed using your user ID.
- You must maintain the confidentiality of your password.
- You should not use the "Remember Password" feature on any websites or applications.
- You should not write passwords down and store them anywhere including on hardcopy documents or in digital files on any computer system.
- If your account or password is suspected to have been compromised, you should report the incident to your contact person at PMB and change the affected password.

2. ACCESS CONTROL

SCENARIOS

1.

Q You have received a hardcopy report from PMB labelled as “Highly Confidential”. What should you do to protect the confidentiality of the said report?

A ***You should store PMB’s hardcopy report in a secured location that is only accessible by authorised individual. Subsequently, you should shred the document properly when it is no longer in use and not required for retention.***

2.

Q As PMB’s appointed vendor, you have been granted access to PMB’s system and was issued with a unique User ID. Your colleague who was not assigned with a User ID requested you to share your User ID and password to extract some PMB’s information to complete his task. Can you share your account with your colleague?

A ***No, you should maintain the confidentiality of your User ID and password as your User ID is only designated for your own usage. Further, you will be held accountable for all activities carried out using your User ID.***

If your colleague requires access to PMB’s system, you should communicate this matter to your contact person at PMB to request for a new User ID to be issued for your colleague.

3.

Q You are using your personal IT device to access PMB’s information from your email account. What can you do to ensure the security of PMB’s information?

A ***You are recommended to set a strong password or biometric authentication to protect your personal IT device from unauthorised access by other individuals.***

4.

Q Upon receiving a unique User ID and password from PMB to access PMB’s system to render your services, what should your immediate action be?

A ***You should immediately change the default password. It is pertinent for you to set a strong password based on recommendation on page 18 of this IS Guide and change it periodically to prevent any unauthorised access.***

Kindly note that these scenarios have been designed purely for education and training purposes and do not make reference to or resemble any real incidents in the past or present

GENERAL

In carrying out your daily tasks, you may be required to share information internally and externally with many parties on various platforms. It is critical that you ensure any information you share is accurate, secured and limited to the intended audience.

OVERVIEW OF INFORMATION SHARING

This section provides you with guidelines, considerations and precautions for you to consider prior to sharing information internally and externally across various platforms. The following is an overview of the areas covered under this section:

AREAS OF INFORMATION SHARING

1 Sharing of information internally and externally via various platforms

- **A** Internal
- **B** External

2 Specific examples and guidelines for sharing information through messaging application and social media

- **A** Messaging Applications
- **B** Personal Social Media

3. INFORMATION SHARING

1 SHARING OF INFORMATION INTERNALLY AND EXTERNALLY VIA VARIOUS PLATFORMS

SHARING INFORMATION INTERNALLY

In instances where you need to collaborate with the members of your working team or within your company to complete a certain task for PMB, you may need to share PMB's information with them. Hence, you should observe the following:

SHARING INFORMATION EXTERNALLY

In instances where you receive a request from an external party (i.e. outside of your working team and company) for PMB's information, you may be required to share the same. As such, you should observe the following:

Within your working team & company

- You should be aware of how the information will be used by the intended audience.
- You should only share information with relevant members in your working team or company on a need-to-know basis.
- If necessary, only share information if you are authorised by your superior.

External parties

- You should be aware of how the information will be used by the intended audience.
- You should inform and obtain consent from PMB before sharing information with external parties.
- You should avoid from sharing information more that what is requested/ required by requestor.
- If necessary, only share information if you are authorised by your superior.

2 SPECIFIC EXAMPLES AND GUIDELINES FOR SHARING INFORMATION THROUGH MESSAGING APPLICATION AND SOCIAL MEDIA

INFORMATION SHARING VIA MESSAGING APPLICATION

In instances where you need to communicate PMB's information swiftly, you may use your personal messaging application (e.g. WhatsApp) to provide and obtain immediate response. Hence, you should observe the following:

Messaging Application

- You should understand the purpose of information request.
- If you are sharing information internally with your working team or colleague, ensure that they are authorised to have access to PMB's information.
- If you are sharing externally with other parties, ensure consent is obtained from PMB's prior to sharing.
- You should send the message to the right recipient only.
- You should be mindful of the members of a group chat and make sure that the members are required to have access to the information.
- You should not share information beyond what is requested.
- If necessary, only share information if you are authorised by your superior.

INFORMATION SHARING VIA SOCIAL MEDIA

In instances where there is any current information or development by PMB, you may be interested to share such information on your social personal media. As such, you should observe the following:

Social Media

- Ensure that you are not sharing PMB's "Highly Confidential" or "Restricted" information without PMB's consent.
- When sharing PMB related information, please ensure that it is from a verified, reputable or official source.
- When sharing picture/ video while working, please ensure that there is no PMB's sensitive information visible in the picture/ video.
- If you have any concerns or grievances about any allegation of misconduct in PMB's business transactions, you are encouraged to use PMB's official whistleblowing channel for PMB's investigation.
- You should not use PMB's name and logo to represent any initiative, programme, event, etc. without PMB's written approval.

3. INFORMATION SHARING

SCENARIOS

1.

Q As the main representative from your company in a collaboration project with PMB, PMB have shared with you some “Highly Confidential” and “Restricted” information. Can you share this information with your team members to perform a feasibility study?

A ***Yes, you may share PMB’s information with your relevant team members on a need to know basis. Nevertheless, you and your team should protect the confidentiality of the PMB’s information.***

2.

Q You have been appointed by PMB as a design and build contractor to undertake an office expansion project. To complete this project, you have appointed a few consultants to assist you. Can you share information received from PMB with your appointed consultants?

A ***Yes, you may share PMB’s information with your consultants once you have obtained consent from PMB. Nonetheless, you are accountable to ensure that your consultants maintain the confidentiality of PMB’s information.***

3.

Q As a PMB’s consultant involved in the designing of a new Rest and Service Area (“RSA”) in North-South Expressway, you are added to a WhatsApp group chat with a few of PMB personnel for ease of communication. You have received a message from the group chat on the launch date for the said RSA. Can you share the good news with your friends and family?

A ***No, you may not share such information with your friends and family until it has been announced publicly by PMB. You are responsible to maintain the confidentiality of all information shared and discussed in the group chat. Hence, you should not share any PMB’s information from the group chat to other external parties without PMB’s approval.***

4.

Q You received a forwarded message from WhatsApp that a new interchange in North-South Expressway near your hometown will be constructed. As you are excited about this news, you would like to share it on your Facebook account. What should you do?

A ***Before sharing on your Facebook, you should verify the accuracy of the information that you received to ensure that it is from a verified, reputable or official source.***

Kindly note that these scenarios have been designed purely for education and training purposes and do not make reference to or resemble any real incidents in the past or present

QUERIES AND INCIDENT REPORTS

How can we help you?

Describe your issue

WHAT TO DO IF YOU HAVE QUERIES ABOUT THIS IS Guide?

You should always feel free to seek clarification regarding this IS Guide with your key contact person at PMB.

WHAT TO DO IF YOU HAVE ENCOUNTERED OR SUSPECTED THAT A BREACH OF PMB'S INFORMATION SECURITY HAS OCCURRED?

If you would like to report a breach of PMB's information security, you should inform your key contact person at PMB or PMB's Compliance and Integrity ("C&I") Function the soonest possible at compliance@plus.com for PMB's attention and further action.

In the event of a personal data breach, please immediately notify the designated Data Protection Officer ("DPO") for the relevant entities listed below:

- Projek Lebuhraya Usahasama Berhad: DPO@plus.com.my
- JustGo Digital Berhad: DPO@justgo.com.my
- Other PMB Group of Companies: compliance@plus.com.my

WHAT IF PMB HAS ENCOUNTERED OR SUSPECTED THAT A BREACH OF YOUR INFORMATION SECURITY HAS OCCURRED?

If the above occurred, PMB will take the necessary measures to mitigate the possible damage in result of the breach of information security incident and inform you the soonest possible for your attention and further action.

PMB reserves the right to amend this IS Guide at any time