PLUS MALAYSIA BERHAD

INFORMATION SECURITY POLICY & GUIDE (PERSONNEL)

June 2024

CONTENT

TERMINOLOGY, ABBREVIATION & DEFINITION

For the purpose of this Information Security Policy & Guide (Personnel) ("ISPG"), the terms used are defined as follows:

No.	TERMINOLOGY/ ABBREVIATIONS	DEFINITION
1.	Authorised Third Party	refers to PMB's contractors, agents, third-party suppliers or service providers with whom PMB enters into an agreement.
2.	BF	refers to PMB's business functions
3.	CC	refers to Corporate Communications Function
4.	C&I	refers to Compliance and Integrity Function
5.	CTO	refers to Chief Technology Officer
6.	Cybersecurity	refers to Cybersecurity Function
7.	Data User	refers to the end user who is authorised to use information
8.	DIS	refers to Digital Initiative Studios Function
9.	HOD	refers to Head of Business Function
10.	HODiv	refers to Head of Division
11.	HRR	refers to Human Resource Relations Function
12.	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).
13.	ISPG	refers to this Information Security Policy & Guide (Personnel), unless stated otherwise.
14.	IT Device	refers to any information technology devices including stationary and mobile devices including but not limited to desktops, laptops, mobile phones and tablets.
15.	Manager	refers to Head of Unit
16.	MD	refers to Managing Director
17.	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.
18.	Personal Data	refers to personal information that an individual has provided to PLUS or made available to PLUS due to his/her business transaction/ contract/ application for jobs, contracts, programmes or products under PLUS, that relates directly or indirectly to the data subject, who is identifiable from that information, including any Sensitive Personal Data.
19.	PMB	refers to PLUS Malaysia Berhad and its related, associated or affiliated companies, including entities within the PLUS Group of Companies such as Projek Lebuhraya Usahasama Berhad, Lebuhraya Pantai Timur 2 Sdn. Bhd., Teras Teknologi Sdn. Bhd., Teras Control Systems Sdn. Bhd., Terra PLUS Sdn. Bhd. and Zoom Interactive Sdn. Bhd. (collectively hereinafter referred to as "PMB", "we", "us" or "our").

TERMINOLOGY, ABBREVIATION & DEFINITION

For the purpose of this ISPG, the terms used are defined as follows:

No.	TERMINOLOGY/ ABBREVIATIONS	DEFINITION
20.	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's Board of Director (including executive and non-executive) (hereinafter referred to as "you" or "your").
21.	RMC	refers to Record Management Centre
22.	RPMS	refers to Rewards, Performance Management & Services Function
23.	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.
24.	TAB	refers to Talent Acquisition & Branding Function
25.	Toll	refers to Toll Function
26.	VPN	refers to Virtual Private Network which encrypts internet traffic and disguise user's online identity to make it difficult for third parties to track user's online activities and steal data.

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:

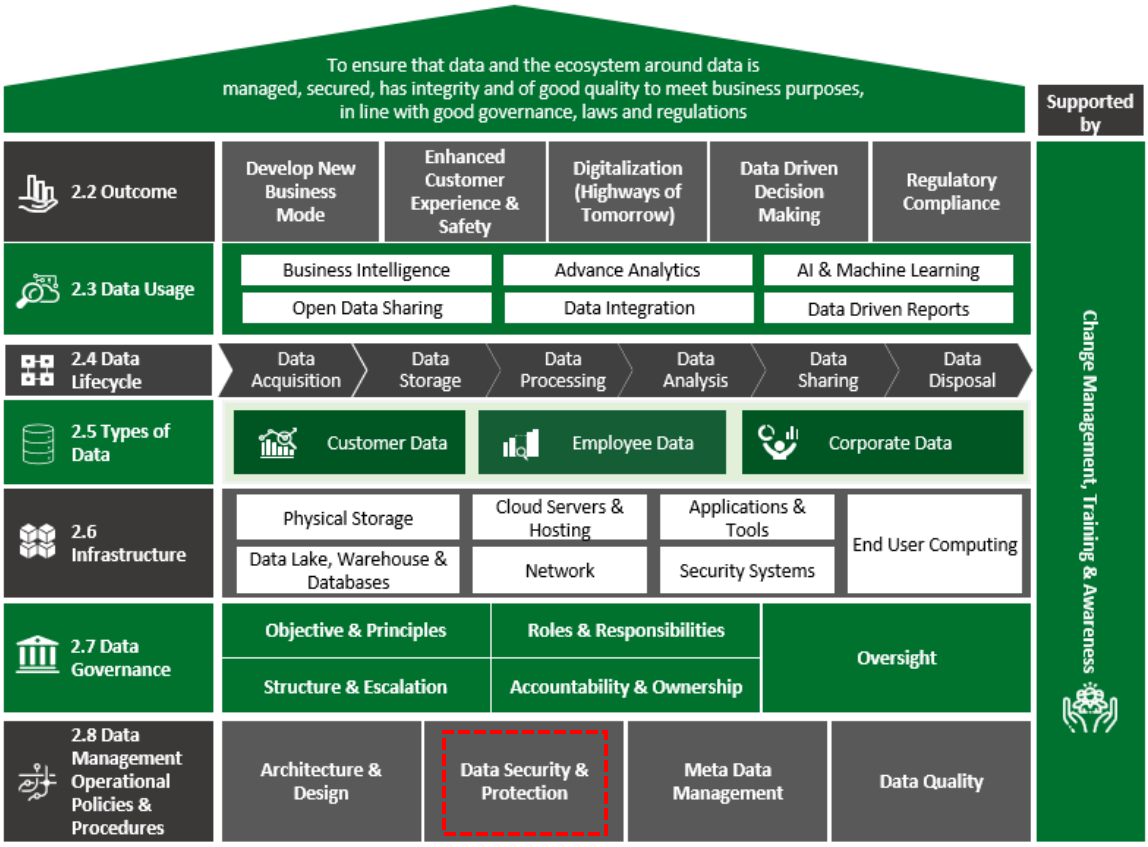


Table 1: Data Governance Framework

To ensure that the governance of data security and protection for PMB's information and other third party's information provided to PMB is 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, digital and physical are secured and protected against internal and external threats.

To achieve the above-mentioned principles, an Information Security Policy & Guide (Personnel) ("ISPG") was developed to provide guidance for PMB Personnel in carrying out their roles and responsibilities in ensuring PMB's information is secured.

PMB'S POSITION ON INFORMATION SECURITY

INFORMATION SECURITY POLICY & GUIDE (PERSONNEL) ("ISPG")

As PMB is committed to uphold the data governance key principles on data security and protection, the ISPG was developed to provide direction for all PMB Personnel on information security controls. This is to ensure necessary measures are undertaken to protect information involved in its day-to-day business activities in reducing information security related risks and defending against internal and external threats throughout the six (6) stages of data lifecycle as follows:

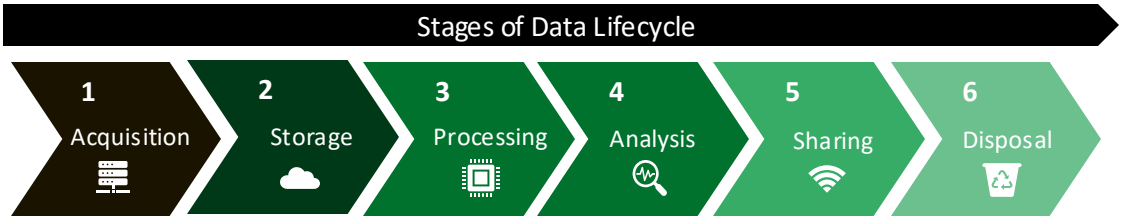


Table 2: Six (6) Stages of Data Lifecycle

The controls embedded within the ISPG prescribe the requirements to maintain an adequate level of security for both physical and digital date which are to be complied by all PMB Personnel to ensure PMB's information is classified and protected against any unauthorised access, usage, disclosure, disruption, modification and destruction.

The ISPG was developed in line with:

- Good governance practices;
- Key areas under ISO 27001 (Information Security Management); and
- Personal Data Protection Act 2010 [Act 709].

The ISPG provides real life examples, dos and don'ts and its consequences to ease PMB Personnel comprehension to apply information security measures as per the ISPG's throughout the six (6) stages of data lifecycle.

There is a tailored Information Security Guide (Third Party) governing all parties formally engaging with PMB including request for PMB's information. Third parties include the following:

- **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 formally engaging with PMB** or have intentions to engage with PMB in the future.
- **Any party requesting for PMB's information** including for academic research, publications, etc. this may include Government agencies, universities, research companies etc.

PMB'S POSITION ON INFORMATION SECURITY

OBJECTIVE

This ISPG is targeted to achieve the following objectives:

To guide you in taking precautionary measures and controls to ensure that both PMB information as well as information received from third parties is adequately protected and secured against security related risks.

FURTHER AMENDMENTS

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

QUERIES

If you have any questions or concerns, please consult Compliance and Integrity ("C&I"). Refer to the last page of this ISPG for C&I's contact details.

ADDITIONAL POLICIES

Information in this ISPG and should be read together with the following:

- PMB Data Governance Framework
- PMB's Privacy Policy and Notices
- PMB's Employees' Code of Conduct
- PMB IT Operations & Management Policies

The above documents are only available for reference to PMB Personnel.

WHO DOES THIS ISPG APPLY TO?

ALL PMB PERSONNEL

- This ISPG applies to both PMB Board of Directors (executive and non-executive) and its employees (permanent and on contract) ("**PMB Personnel**"), regardless of their position or role.
- All PMB Personnel must comply with this ISPG, other PMB's policies, procedures, processes and all applicable laws in the course of employment.
- Head of Business Functions ("**HOD**")/ Head of Business Units ("**Manager**") are responsible to communicate and ensure compliance to this ISPG within their respective business functions/ units.

WHAT IS YOUR RESPONSIBILITY?

READ AND COMPLY

You must read, understand and comply with this ISPG.

Any exception to this ISPG would require consent from the Managing Director ("MD").

PROTECTING PMB'S INFORMATION

It is your responsibility as PMB Personnel to protect PMB's information, both hardcopy and digital format throughout the six (6) stages of data lifecycle against information security related risks by implementing the necessary controls and mechanism as provided under ISPG. Your adherence and compliance to these controls are necessary in ensuring PMB's information are secured through out the six (6) stages of data lifecycle.

PROTECTING INFORMATION PROVIDED TO PMB

It is also your responsibility as PMB Personnel to safeguard Third Party information that has been provided to you including securing and protecting against any unauthorised access, usage, disclosure, disruption, modification and destruction as well as preserving the confidentiality and integrity of their information.

PROTECTING PMB'S INFORMATION PROVIDED TO THIRD PARTIES

It is your responsibility to ensure that all **third parties** are aware of the Information Security Guide (Third Party) requirements.

LEAD BY EXAMPLE

PMB Top Management, HODs and Managers must demonstrate good tone from the top and communicate this ISPG to their team members.

PMB Top Management, HODs and Managers must show respect and maintain open, honest and constructive two-way communication with their team members. This means encouraging them to ask questions, make suggestions and raise concerns or report possible violations of this ISPG.

UNDERSTAND THE CONSEQUENCES

If you fail to comply with this ISPG, including non-completion of trainings relating to information security, it will result in disciplinary action, up to and including termination of employment or dismissal.

Any violation to this ISPG may also result in damage to PMB's reputation and financial prospect.

INFORMATION SECURITY POLICY STATEMENTS

POLICY STATEMENTS

GENERAL

- **All PMB Personnel** shall **comply** with this ISPG and any exception required must be consented by the approving authority.
- **Protect** PMB's information and information provided to PMB against **internal and external threats** through the implementation of appropriate **security controls.**
- Assess and manage **information security related risks** regularly through adequate governance, technology and infrastructure.
- PMB reserves the right to take **disciplinary** or **legal action** against the perpetrator who caused a breach to PMB's information, systems, services or applications.

ORGANISATION FOR INFORMATION SECURITY

- **All PMB Personnel** are **responsible** to ensure information, either in hardcopy or digital form are managed, handled, used, shared and disposed in accordance with this ISPG.
- Provide adequate **training, awareness and engagement programmes** on information security to PMB Personnel.
- Ensure adequate information security controls are in place with **periodic review** and **internal audits.**

INFORMATION CLASSIFICATION

- **Classify PMB's information** and **information received from third parties** in accordance with PMB's information classification criteria.

INFORMATION LABELLING AND HANDLING

- **Label** and **handle** all information in a secured manner according with this ISPG.
- **Retain** information for the duration permitted/ required by PMB's procedures and any relevant Malaysian laws.
- **Dispose** information that is no longer required, usable or relevant in a secured manner.
- Undertake necessary security measures to avoid information security breaches on personally owned or PMB issued **IT devices**.

ACCESS CONTROL

- Restrict access to physical and digital information to **authorised personnel** based on a **need-to-know basis** and **least privilege** only.
- Ensure **segregation of duties** in managing access control and information is not used and processed beyond its **intended purpose.**
- PMB reserves the **right** to block or remove access to certain internet websites, domain and other IP addresses which are not specifically related to official business use.

INFORMATION SHARING

- Ensure information shared internally and externally is **accurate**, **secured** and limited to its **intended purpose** and **audience**.
- Obtain **appropriate authorisation** prior to sharing information.
- Ensure information is only shared via **secured** and **approved platform**.
- Exercise **due care** and undertake necessary **precautions** when sharing information in line with the guidance provided in the ISPG.

KEY HIGHLIGHTS OF INFORMATION SECURITY POLICY & GUIDE

GENERAL

This ISPG will be focusing on 5 key areas of information security for your ease of reference and implementation.

KEY HIGHLIGHTS

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

1 **Organisation for information security** 	What are your roles and responsibilities as a **Data Owner**, **System Owner**, **Data User** and **as a supporting business functions ("BF")** to ensure information are secured.
2 **Information classification** 	What are the **four (4) information classification categories and** how you should classify a document containing **several information classifications**, **change** information classification, classify **information from third parties**, **review** and **update** information classification.
3 **Information labelling and handling** 	How you should label and handle **documents**, **information mediums**, **printing**, **storage**, **filing**, **backup**, **retention** and **disposal** as well as protecting information while working at the **office or home**.
4 **Access control** 	How you can ensure secured access control when accessing **filing rooms**, **PMB's systems** and **end-user computing**.
5 **Information sharing** 	What are the security measures you should take when sharing information **internally**, **externally**, using **messaging application** and **social media**.

UNDERSTANDING DATA LIFECYCLE

GENERAL

As a PMB Personnel, you will be dealing with PMB's information from the point it is acquired until it is eventually archived or disposed. Hence, it is important for you to understand the information security measures to be practised throughout the six (6) stages of data lifecycle.

STAGES OF DATA LIFECYCLE

To know the relevant areas of information security to be practised under each stage of data lifecycle, you may refer to the following:

Stages of Data Lifecycle		Information Security Areas
Acquisition	Creation and collection of data gathered/ captured from one or multiple sources point.	2 Information classification 3 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.	2 Information classification 3 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.	3 Information labelling and handling 4 Access control
Analysis	Inspecting, cleansing, transforming and modelling data with the goal of discovering useful information, informing conclusions and supporting decision making.	3 Information labelling and handling 4 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.	3 Information labelling and handling 5 Information sharing
Disposal	Deleting, retiring and destroying data stored on all storage medium when data reaches its end-of-life or relevancy.	3 Information labelling and handling

1. ORGANISATION FOR INFORMATION SECURITY

GENERAL

In carrying out your daily tasks, you will be dealing with different types of PMB's information. To ensure that PMB's information is being given adequate protection, you may be assigned with different roles and responsibilities prior or upon commencement of any task or exercise.

WHO ARE THE KEY PERSONNEL?

Since you have to deal with PMB's information to complete your workload on a daily basis, you are all deemed as **Data Users**. To ensure proper organisation of information security, some of you may also be assigned with additional role and responsibilities as a **Data Owner** or **System Owner**. Hence, you must be aware of **who are assigned** with these roles and **what are your responsibilities** as follows:

	Data Owner	System Owner*	Data User
Who can be assigned?	**HOD**	**HOD/ Head of Unit** or assigned by the Head of Division ("HODiv")*	**PMB Personnel** who are authorised to use the information
What are your responsibilities?	• **Manage information** under your purview. • **Determine** the following: ✓ appropriate information classification level; ✓ information usage; ✓ authorised personnel and/or any other parties to have access to your information; ✓ Information storage location; and ✓ security measures used to protect the information.	• **Manage the operations and identify security requirements** of systems, applications/ software and services, including proper maintenance and security controls. • Review and **approve** system, application or software requirement changes. • Facilitate **annual system security risk assessment**. • **Implement adequate security** measures and ensure compliance with security policies, standards, practices and procedures.	• Ensure **usage and access to information** comply with this ISPG. • To **share information** only upon obtaining approval.

**Note: There should only be one System Owner for a particular system. However, for exceptional instances where a system is managed by more than one (1) BFs, joint system owners can be appointed but this does not dissolve your responsibility as a System Owner.*

1. ORGANISATION FOR INFORMATION SECURITY

WHO ARE THE SUPPORTING BUSINESS FUNCTIONS?

You are not alone in performing your responsibilities as a Data User, Data Owner and System Owner. The following BFs will assist and support you in protecting information security and complying with this ISPG:

HUMAN RESOURCE

Necessary information security measures are to be taken throughout the three (3) stages of employment as follows:

Prior to employment

TAB shall be responsible to ensure the following:

- To perform employment and qualification reference checks on all candidates prior to employment;
- That successful candidates are to agree and sign the terms and conditions of their employment contract, including their responsibilities regarding information security; and
- The candidates' personal data collected during the employment process shall be protected in line with this ISPG, Privacy Policy and Notices, Personal Data Protection Act 2010 [Act 709] and any other applicable laws.

During employment

RPMS/ HRR shall ensure relevant parties are notified and access removed/ adjusted upon PMB Personnel change in role (i.e. promotion, demotion, transfer of department, etc.) or suspension.

Upon resignation or termination

RPMS shall be responsible to manage employment termination or offboarding process, including ensuring relevant parties are notified, access removed/ adjusted upon resignation/ termination of employee and payroll termination/ offboarding process is adhered to.

COMPLIANCE AND INTEGRITY

C&I will assist you with any queries relating to this ISPG and provide guidance to you in implementation of this ISPG.

C&I will work with Cybersecurity and DIS to cultivate knowledge and awareness on information security threats and best practices by conducting regular training to all PMB Personnel and developing communication material to be disseminated throughout the organisation.

In ensuring applicability and relevancy of information in this ISPG, C&I will review and update the same every five (5) years or when the environment changes to ensure its continuing suitability, adequacy and effectiveness.

CYBERSECURITY & DIS

Cybersecurity will act as the enabler to execute and implement information security measures throughout PMB.

Cybersecurity will work with you to coordinate with relevant authorities and specialists to improve knowledge of best practices on information security.

Cybersecurity and DIS will coordinate with you to ensure that audit findings from information security audit are addressed and rectified in a timely manner.

Cybersecurity and DIS will assist you should you have any difficulty or concern on PMB's IT device and system.

1. ORGANISATION FOR INFORMATION SECURITY

WHO ARE THE SUPPORTING BUSINESS FUNCTIONS?

INTERNAL AUDIT

Internal Audit and other appointed external auditors will carry out regular information security audit or as directed by the Management/ Board to ensure compliance with this ISPG.

What to do if you have encountered or suspect a breach of information security has happened?

	Technical Incident	Non-Technical Incident
Description	Technical incidents may involve phishing, hacking, malware, password attacks, Denial of Service (DOS), man in the middle, ransomware, password attack etc.	Non-technical incidents may involve accidental sharing of wrongly classified information, unauthorised information sharing, losing important hardcopy documents etc.
Contact	You should contact DIS via DIS Helpdesk System (DISHES), email at helpdesk.dis@plus.com.my, Microsoft Teams (Digital Initiative Studio Helpdesk) or via phone call at 03-7666 4041/ 4048.	You should contact C&I via email at compliance@plus.com.my

WHAT ARE YOUR RESPONSIBILITIES AS PMB PERSONNEL?

Being a Data Owner, System Owner and Data User, you must consider the following before dealing with PMB's information:

Do's
you SHOULD

- ✓ Understand your role and responsibilities as a personnel and BF in ensuring information security.
- ✓ Carry out your responsibilities in accordance with this ISPG.

Don'ts
you SHOULD NOT

- ✗ DO NOT deal with PMB's information without understanding your role in information security.
- ✗ DO NOT neglect your responsibilities in accordance with this ISPG.

1. ORGANISATION FOR INFORMATION SECURITY

SCENARIOS

1.

Q As an Insurance & Claims Management Executive, you receive personal information of customers who file for accident claims. In order to analyse and process the claim, you are required to obtain information from TMC, customer and insurance provider. How should you handle the information?

A ***You are a Data User as you receive internal and external information. Hence, you should ensure adequate measures are in place to protect the security of the information when using, accessing and sharing the information.***

2.

Q As a Head of Operations Excellence, you plan to take two weeks of annual leave. You have discussed with your superior to delegate your responsibilities as a Data Owner to your subordinates during your absence. Is this practice allowed?

A ***Yes, you are allowed to delegate the role in your absence. However, you are still accountable as a Data Owner.***

3.

Q As a Data Lake System Owner, the Marketing Team approach you to gain access to traffic data in the Data Lake to perform target market analysis. Can you provide access to the Marketing Team?

A ***You are only allowed to provide access upon approval from the designated Data Owner, i.e. Traffic Safety.***

4.

Q In the course of discharging your duty, you were required to share some "Highly Confidential" information with your vendor, following MD's approval. Subsequently, you notice that the "Highly Confidential" information was circulated on Facebook. What do you do?

A ***This is a breach of information security which requires immediate attention. Hence you should contact your HOD and C&I for advice on the next course of action.***

5.

Q You open an email attachment sent by a third party and notice an unknown programme is running in your PMB issued laptop. What do you do?

A ***You should disconnect your PMB issued laptop from any network/ wifi and contact DIS immediately for their assistance.***

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. INFORMATION CLASSIFICATION

GENERAL

In your daily tasks, you will receive many information from various sources which may include internal and external information. If an information is under your purview, you need to classify it accordingly based on the need, priority, protection necessary and impact of unauthorised information sharing to ensure that the information is safeguarded with optimum level of controls in place.

If you receive information from any third parties, you must be aware of their information classification. You must also consider whether PMB is restricted from sharing third parties' information under any contracts to ensure information confidentiality. This is important to determine whether you may share such information with other PMB Personnel or external third parties.

OVERVIEW OF INFORMATION CLASSIFICATION

In this section, you will be guided on how to classify any information that is under your responsibility and purview. The following is the overview of the areas covered under this section:

AREAS OF INFORMATION CLASSIFICATION

1. **Information Classification**
   - A. **Types of information classification**
   - B. **Information classification upgrade and downgrade**
   - C. **Classifying information received from third parties**
2. **Frequently Asked Questions**
   - A. **Blanket approval**
   - B. **Classifying document containing different information classifications**

2. INFORMATION CLASSIFICATION

1 INFORMATION CLASSIFICATION

A INFORMATION CLASSIFICATION LEVEL

To begin working with any information, you must understand that all PMB's information is considered as **sensitive** and must be protected from unauthorised access and sharing. There are 4 levels of information classification based on its sensitivity as follows:

	Highly Confidential	Restricted	Internal	Public
Information criteria	• Information that is strictly on a **need-to-know basis**. • This Information is considered **HIGHLY SENSITIVE** and will have **reputational or financial** implication.	• Information that is **restricted** to selected personnel within PMB. • This information **MAY BE SENSITIVE** or may have a **reputational or financial** implication.	• Information for **internal consumption** and intended to be shared internally among PMB Personnel only.	• Information for **public knowledge**.
Approval before sharing (internal & external)	• You must obtain **approval** from HODiv for internal sharing and the **MD** for external sharing.	• You must obtain **approval** from **HOD** for internal sharing and **HODiv** for external sharing.	• You must obtain **approval** from **HOD** for external sharing.	• You must obtain approval based on level of risk: ✓ **Low risk:** Consult and obtain approval from **HOD** ✓ **High risk:** Channel through CC (if required, consult other relevant BF as well), to be reviewed and approved by relevant **C-Suites/ MD**. • After approved, information can be shared publicly without restriction.
Example of document*	• Concession Agreement • Disciplinary Management Committee Report/ Whistleblowing Report • Financially/ commercially sensitive information	• Audit report • Board Paper • Discretionary Authority Limits • Annual Operating Plan • Meeting minutes • Corporate risk register • HR related information • Customer data • Toll data • Tender information	• Internal emails between PMB Personnel • Code of Conduct • All policies and procedures • Organisation chart • Information on PLUS lounge • Announcement via corporate email	Information released on: • Official website • Official social media • Press release • Official announcements • Interviews • Travel time advisory • Chatbot and PLUS Applications • Product flyer/ brochure

Note:

** The examples listed under each information classification are non-exhaustive and based on HOD's discretion.*

If you are unsure on the proper classification for a document/ information, you should confirm with your HOD on the appropriate information classification level.

2. INFORMATION CLASSIFICATION

1 INFORMATION CLASSIFICATION

B INFORMATION CLASSIFICATION UPGRADE AND DOWNGRADE

As time passes by, there might be situations which make it necessary for an information classification to be upgraded or downgraded. In such situations, you may change an information classification for an information/ document by fulfilling the following requirements:

	Classification upgrade	Classification downgrade
Criteria	The information has fulfilled the criteria of the new information classification category.	The information has lost its sensitivity or a situation requires its classification to be downgraded.
Approval	You must obtain approval from **HOD**.	
After approval	• **You** must update the information classification label on the affected document. The document must be treated and protected based on the new information classification. • **HOD** must notify all affected parties on the change to information classification for a document within an appropriate amount of time from the date of approval.	

You can only upgrade, or downgrade information classified as “Restricted” or “Internal”. For “Highly Confidential” information, it must be disposed if it is no longer usable or relevant.

APPLICATION

Scenario 1: A proposal classified as “Restricted” has been reviewed and now contains details that are financially sensitive. It should be upgraded to “Highly Confidential”.

Step 1	Step 2	Step 3
You should obtain approval from your HOD to upgrade classification level.	You should update the information classification label and protection level of the document.	HOD should notify all related parties of the revised classification level.

Scenario 2: A job vacancy announcement classified as “Internal” is now to be announced to the public for external candidates. It should be downgraded to “Public”.

Step 1	Step 2	Step 3
You should obtain approval from your HOD to downgrade classification level.	You should update the information classification label.	HOD should notify all related parties of the revised classification level.

2. INFORMATION CLASSIFICATION

1 INFORMATION CLASSIFICATION

C CLASSIFYING INFORMATION RECEIVED FROM THIRD PARTIES

WHAT SHOULD YOU DO WHEN YOU RECEIVE THIRD PARTY'S DOCUMENT?

IF A THIRD PARTY DOCUMENT HAS BEEN LABELLED IN ACCORDANCE WITH THE THIRD PARTY'S STANDARD

You should consider the following to determine the level of security controls to put in place for that document:

Scenario 1: The third party has provided **instruction or guideline** on how to protect their information or there is an **agreement/ contract** which states PMB's obligation to protect third party's information.	You should **follow such instruction, guideline or agreement/ contract** in order to determine the level of protection necessary for a document.
Scenario 2: The third party has not provided any **instruction or guideline and** there is no **agreement/ contract** stating how PMB is obligated to protect third party's information.	You should **align it with PMB's information classification** that have a similar criteria and level of protection inline with our ISPG.

IF A THIRD PARTY DOCUMENT HAS NOT BEEN LABELLED WITH ANY INFORMATION CLASSIFICATION

You should refer to **PMB's information classification** in this ISPG and classify it based on the classification as agreed by your HOD. You should protect that information and handle it based on the information classification.

2 FREQUENTLY ASKED QUESTIONS

Now that you know how to classify information, the following are common questions to further guide you in this process:

A Can you request for a blanket approval from the approving authority to share information?

If you need to share information of the **same nature and purpose routinely** (e.g. traffic flow, accidents and RSAs), a blanket approval can be obtained from the approving authority and individual approval is not required.

B How do you classify a document which contains several information with different information classifications?

If a document contains information with different classification categories, the document should be classified based on the **highest level of classification** of the information contained in the document.

2. INFORMATION CLASSIFICATION

To ensure that your information is properly classified, you must consider the following:

- ✓ **Classify all information/ document** including work in progress document.
- ✓ When you receive information/ document from other BFs or third parties, you must **handle and protect the information** in accordance with its information classification.
- ✓ Consider the **criteria of information, risk of disclosure and level of protection** required to determine the appropriate information classification.
- ✓ For information received from third parties, classify the information based on contractual obligation or similar **classification labelled by third parties**.
- ✓ BF are recommended to keep, maintain and update an **information inventory** to keep track of information dealt with and shared.
- ✓ If information shared has been labelled with the **wrong information classification**, retrieve the information, classify and label it with the correct information classification.
- ✓ **Review** information classification as and when required to ensure accurate classification and information is always protected.

- × DO NOT share information internally or externally before **properly classifying and labelling** information/ document.
- × If information shared has been labelled with the wrong information classification, DO NOT **leave information unretrieved**. This is to prevent further mistreatment of the information.

2. INFORMATION CLASSIFICATION

SCENARIOS

1.

Q You are tasked to prepare an update report to Management on Land Gazetting. How do you classify it?

A ***Firstly, you need to establish who would be the audience for this report and determine the sensitivity of the information to be shared as guided by page 17 of this ISPG. For this specific example, the report may be classified as "Restricted" if it requires input from various BFs and the information is not highly sensitive.***

2.

Q You receive a DMPU email with an announcement that a senior officer at PMB has been accorded with a royal title. Subsequently in the day, you notice the same information posted on PMB's Facebook. As you are excited to share this information with your friends and family, can you share the DPMU or Facebook posting?

A ***DMPU information is classified as "Internal" whereas PMB's Facebook post is classified as "Public". As such, you should not share the DMPU announcement but you can share the PMB's Facebook posting.***

3.

Q Section Office has shared a report to you. While browsing through the report, you notice that it was wrongly labelled as "Internal" as opposed to "Restricted" as the report contains information that should not be distributed widely across PMB. What should you do?

A ***You should inform the sender to retrieve all report distributed, classify and label it with the correct information classification prior to redistribution.***

4.

Q While you were drafting an email to circulate a "Highly Confidential" Whistleblowing report to senior management, you accidentally included a third party's email address. You realise this mistake after sending out the email. What do you do?

A ***You must inform your HOD of the situation immediately. You and your HOD must put in the best effort to retract the information such as using the "recall" function in the email and contact the email recipient to delete the information.***

Q **5.**

You have signed a data sharing agreement with a Business Partner which requires you to exercise due care in ensuring the confidentiality of data shared. In the last few months, you have been receiving PLUS highway customer data from the Business Partner. How should you classify this information?

A ***If the agreement provides a standard for information classification, you should comply with the standard provided. However, if there is no standard provided in the agreement, you should classify the customer data in accordance with PMB's information classification that aligns with the information security requirements under the agreement.***

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.

3. INFORMATION LABELLING AND HANDLING

GENERAL

Once information is classified, you must ensure that information is labelled and handled in line with its classification. Let us walk you through some of the considerations you need to bear in mind in handling and labelling information.

OVERVIEW OF INFORMATION LABELLING AND HANDLING

In this section, you will be guided on how to handle and label any information that is under your responsibility and purview. The following is the overview of the areas covered under this section:

AREAS OF INFORMATION LABELLING AND HANDLING

1. **Information labelling**
   - A. Labelling with information classification
   - B. Incorporating confidentiality statement
2. **Information handling**
   - A. Medium of information sharing
   - B. Printing, storing, filing & disposal
   - C. Backup
   - D. Protecting information while working
   - E. Usage of IT devices

3. INFORMATION LABELLING AND HANDLING

1 INFORMATION LABELLING

A LABELLING WITH INFORMATION CLASSIFICATION

Before sharing any information/ document with any parties, you should ensure that it has been labelled with its information classification according to the following requirements:

	Highly Confidential	Restricted	Internal	Public
Applicability	It is **compulsory** for you to label every "Highly Confidential" information.	It is **highly encouraged** for you to label "Restricted" and "Internal" information.		No requirement for labelling.

Once you have determined your document's information classification label, you should perform the following:

Hardcopy

- Ensure that hardcopy documents are labelled with its information classification on top right-hand side of the front page of the document.

Digital

- When using Microsoft Word, Excel, PowerPoint or any other digital documents, label the document with its information classification at the "header" on top right-hand side of the document.

B INCORPORATING CONFIDENTIALITY STATEMENT

After labelling the documents based on its information classification, you are recommended to insert a confidentiality statement at the cover/ front page of the document as follows:

> "This document is classified as **HIGHLY CONFIDENTIAL/ RESTRICTED/ INTERNAL** and is solely intended for the recipient it is addressed to. 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."

3. INFORMATION LABELLING AND HANDLING

2 INFORMATION HANDLING

A MEDIUM OF INFORMATION SHARING

When sharing information either by using email, physical mail or fax, you must protect its information security by carrying out the following:

	Highly Confidential	Restricted	Internal	Public
Email	Use internal email system and include confidentiality statement.			No special requirement
Physical Mail	• Use a plain sealed envelope marked with "to be opened by addressee only" on the front and to seal the envelop and mark with a cross at the back. • Hand delivered, sent by registered mail or courier (with confirmation of receipt).			No special requirement
Fax	• Send a test page and require immediate phone confirmation of receipt. • Send the full page and require phone confirmation of receipt.		Keep record of the fax number.	No special requirement
OneDrive/ SharePoint	• Check the intended recipient before sharing files via OneDrive and SharePoint. • Set an expiry date and password when sharing files with external parties via OneDrive and SharePoint.			No special requirement

**Note: Physical mail refers to any mails or correspondences done using hardcopy documents.*

⚠ Caution:
- Do not use OneDrive and SharePoint to store personal information, e.g. personal photos, music and video etc.
- Do not use removable storage media (e.g. external hard disk, USB flashdrive) to store and transfer PMB's information.

3. INFORMATION LABELLING AND HANDLING

2 INFORMATION HANDLING

B PRINTING, STORING, FILLING & DISPOSAL

When printing, storing, filing and disposing information, you must protect information security by carrying out the following:

	Highly Confidential	Restricted	Internal	Public
Printing	• Copying / replication is prohibited. • Issuance of a new document must be documented. • Control copy number to be recorded.	• Limited copies may be made only by permission of **HOD** or his/her designates.	• Limited copies may be made only to PMB Personnel.	• Unlimited, subject to preserving the original content.
Storage	• **Hard copy**: Store in a secured & locked location. • **Electronics files**: Store in a location that requires highest access authentication.	• **Hard copy**: Store in a secured & locked location. • **Electronics files**: Store in a location that requires access authentication.	• **Hard copy**: Store in a location that is inaccessible to public. • **Electronics files**: Store in a location that requires access authentication.	• Retain the original copy prior to public dissemination.
Filing*	• **Hard copy**: Information is placed in a file labelled as HIGHLY CONFIDENTIAL. • **Electronics file**: Information is encrypted.	• **Hard copy**: Information is placed in a file labelled as RESTRICTED. • **Electronics file**: Information is encrypted.	• **Hard copy**: As per RMC's procedure. • **Electronics file**: Information is not accessible to public.	• No special requirement.
Disposal**	• **Hard copy**: Shred immediately using an approved cross-cut shredder when no longer in use.	• **Hard copy:** Shred immediately when no longer in use.	• **Hard copy:** Shred.	• **Hard copy**: No special requirement and it is permitted to be reused as rough paper.
	• **Electronic file:** ➢ Delete and empty Recycle Bin immediately when no longer in use. ➢ Send CDs, DVDs, dead hard drives, laptops, etc. to DIS for degaussing and appropriate disposal.			No special requirement.

Note:
** HOD to ensure that information filing is carried out in line with the Records and Documentation Management Procedures.*
***You must retain PMB's information for the duration permitted/ required by PMB's Records and Documentation Management Procedures and any relevant Malaysian laws.*

3. INFORMATION LABELLING AND HANDLING

2 INFORMATION HANDLING

C BACKUP

To ensure that information is available at all times and to prevent accidental lost of document, you must ensure that the information under your purview are properly backed up as follows:

Hardcopy

- You must ensure that hardcopy documents are scanned into digital form and are properly labelled, inventoried and saved into OneDrive/ SharePoint.

Digital

- You must ensure that digital documents are properly labelled, inventoried and saved into OneDrive/ SharePoint.
- If required, DIS support team shall backup essential business data upon request/ approval from the HOD.

Information in systems and applications

System Owner shall ensure:

- Performance of regular back up of information in PMB's systems and applications.
- Full/ incremental backup of the system's information is performed automatically on the backup server at defined intervals.
- The extent and frequency of backups shall be based on the business and security requirement of the information involved.
- Restoration shall be carried out to check the integrity of the backed-up data and critical information systems shall be tested half yearly.

D PROTECTING INFORMATION WHILE WORKING

Depending on necessity, you may be required to carry out your daily tasks at the office, home or any other suitable locations. Hence, it is important for you to understand how to protect the information you are dealing with while working at different locations as follows:

Working from office

- ✓ When leaving workspace unattended, to 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 confidential matters** in public places.
- ✓ **To obtain authorisation if you are to remove PMB's property** from PMB's premises is necessary.

Working away from office/ home

- ✓ To use PMB issued or personally owned devices that are equipped with **security features**.
- ✓ To keep information in any form in a **secured location**.
- ✓ In transmitting information, to always use PMB issued IT devices or IT equipment with **built-in secured access** authorised by DIS.
- ✓ To **logoff and shutdown** IT devices at the end of the day.

3. INFORMATION LABELLING AND HANDLING

2 INFORMATION HANDLING

E USAGE OF IT DEVICES

As a PMB Personnel, you may be required to use the following IT devices to carry out and complete your job roles and tasks on a daily basis:

I. Personally owned IT devices; and
II. PMB issued IT devices.

This section will provide you with guidance on how to ensure information security while using the above IT devices.

I PERSONALLY OWNED IT DEVICES

HOW TO USE YOUR PERSONALLY OWNED IT DEVICES SAFELY?

To access emails and messaging applications anywhere at any time, you may need to use your own IT devices. If you would like to access your PMB's email account or applications via your personally owned IT device, you will need to obtain authorisation from DIS. Hence, you must observe the following :

Do's
you SHOULD

- ✓ Consult and obtain DIS approval.
- ✓ Personally owned IT devices used to connect to PMB network must be **secured with anti-virus software** and updated regularly.
- ✓ Users must **avoid accessing, forwarding, replying or downloading suspicious emails or websites** to prevent phishing*.

Don'ts
you SHOULD NOT

- × DO NOT use a **"rooted" (Android) or "jailbreak" (iOS) IT device**. This is to avoid the IT device from being vulnerable to cyber attacks.
- × DO NOT engage in **illegal activities** including download, transmit, view or store illegal material including child pornography, fraud, etc.
- × DO NOT use personal email for work related matters.
- × DO NOT connect personally owned IT devices to PMB staff wifi.

⚠ PMB's rights:

- PMB reserves the right to track personally owned IT devices connected to PMB's network and DIS may remove your User Account access when it is deemed necessary.
- PMB reserves the right to introduce and enforce additional security controls as and when it deems appropriate.
- PMB reserves the right to inspect and remove PMB's information from your approved personally owned IT devices upon resignation/ termination.

**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.*

3. INFORMATION LABELLING AND HANDLING

II PMB ISSUED IT DEVICES

HOW TO USE YOUR PMB ISSUED IT DEVICES SAFELY?

While working at the office or at home, you may be provided with PMB issued IT devices such as desktop, laptop or mobile phone to assist you in carrying out your job roles. Hence, you must observe the following:

Do's
you SHOULD

- ✓ You should use PMB's internet in a professional, ethical, responsible and lawful manner.
- ✓ You should only use PMB issued IT devices, systems or email for business activities, and if required for personal use, it must be reasonable.
- ✓ You should enable **scheduled antivirus scan** for PMB issued IT devices.
- ✓ You should only use **pre-approved software** on PMB issued IT devices. If you need to use any other software installation that is not pre-approved, you should provide a business justification and obtain approval from your HOD and DIS.
- ✓ You should always use VPN when connecting to public WiFi.
- ✓ You should ensure that PMB issued IT devices are handled in a secured manner as to prevent lost or stolen information.
- ✓ You should store PMB IT devices securely and out of sight.
- ✓ If any PMB issued IT devices is stolen, you should make a police report and report to DIS.

Don'ts
you SHOULD NOT

- ✗ DO NOT access, forward, reply or download any **suspicious emails or untrustworthy websites** to avoid phishing.
- ✗ DO NOT engage in **illegal or inappropriate activities** including download, transmit, view or store illegal material including child pornography, fraud, etc.
- ✗ DO NOT disable or remove **anti-virus and malware protection software** installed in the PMB issued IT devices under any circumstances.
- ✗ DO NOT access or download software that is **not pre-approved** by your HOD and DIS, including games, games upgrades or unauthorised software.
- ✗ DO NOT duplicate, reproduce or install software **without your HOD and DIS approval**.
- ✗ DO NOT leave PMB issued IT devices in unattended vehicles or public spaces.

⚠ PMB's rights:

- ✓ PMB reserves the right to introduce and enforce additional security controls as and when it deems appropriate. Hence, DIS may remove total access of any IT devices to PMB Corporate Network at any time.
- ✓ PMB reserves the right to monitor stored files, email messages, internet usage and remote access to protect PMB's information, ensuring optimal system performance, maintenance, auditing, and investigation.

3. INFORMATION LABELLING AND HANDLING

SCENARIOS

1.

Q Your personal mobile phone is configured to access PMB's email. Your friend has provided you a link to install an unknown trial application that is NOT AVAILABLE in Google Play or App Store. Can you install it on your personal mobile phone?

A ***No, you should refrain from installing any unknown application which may pose threats to your personal mobile phone including unauthorised access and information leakage from your personal mobile phone.***

2.

Q Upon purchasing a secondhand mobile phone, you discover that it was "jailbreak". Is it permissible to use a "jailbreak" mobile phone to connect to PMB's network?

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 connect to PMB's network.***

3.

Q You are urgently preparing a report and your PMB issued laptop crashed. Can you resume work on your personal laptop?

A ***You should refrain from using your personal laptop as your personal laptop may not have the required security mechanism aligned with PMB's IT policy. In this situation, you should inform your superior and contact DIS for the next course of action.***

4.

Q PMB has issued a mobile phone to you for business use. Your colleague has recommended that you install a TikTok application on your PMB issued mobile phone as it may assist you in obtaining the latest government announcements. Can you install it on your PMB issued mobile phone?

A ***No, you should not install any new application into PMB issued mobile phone. If the application is required, you should consult and obtain approval from your HOD and DIS prior to installation.***

5.

Q Your PMB issued laptop does not have a specific software that you require to complete a task. To resolve this, you are thinking of installing a new software found on Google. Is that allowed?

A ***No, you are not allowed to install unauthorised software on PMB issued laptop. You should consult your HOD and DIS for direction.***

6.

Q While you are working from home, your child would like to attend an online class. Can you allow your child to use your PMB issued laptop to attend the class?

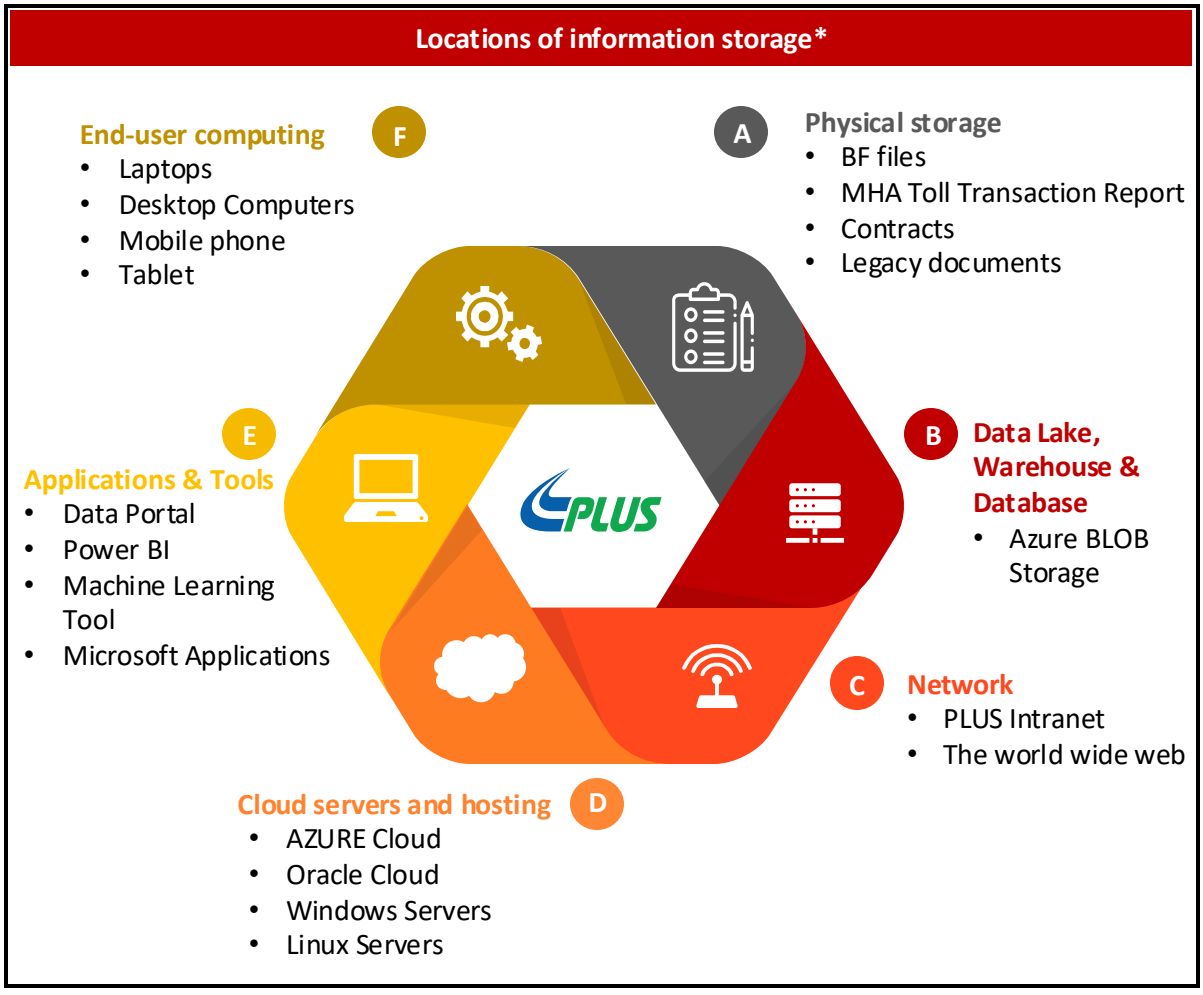
A ***No, PMB issued laptop is a company asset provided to you to complete your work and it is not intended for personal use. By allowing other people to access your PMB issued laptop, you may expose PMB to the risk of information loss due to any intentional or unintentional acts.***

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

4. ACCESS CONTROL

GENERAL

PMB's information is stored in different parts of the organisation including the following:

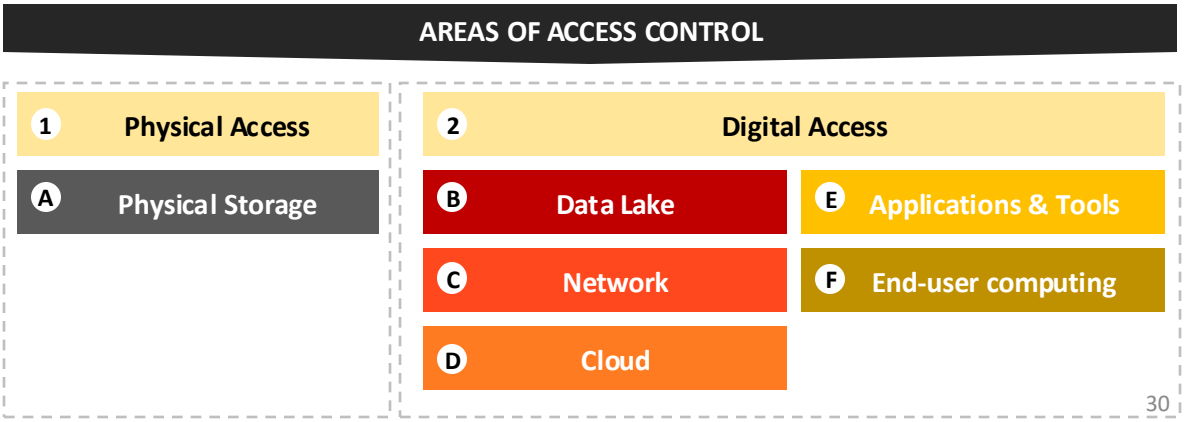


**Note: The locations listed above are non-exhaustive.*

The locations in which the information is stored need to be properly secured by limiting access to authorised personnel only.

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 is the overview of the areas covered under this section:



4. ACCESS CONTROL

1 PHYSICAL ACCESS

A PHYSICAL STORAGE

GENERAL

PMB's information may be stored in PMB's premises and equipment. You are obligated to ensure the security of premises and equipment when accessing PMB's information as follows:

PREMISE SECURITY:

PMB's hard copy information is stored is various locations of the organisation. You are obligated to protect information security at PMB's premises as follows:

Office, rooms and facilities	• You should ensure that offices, rooms and facilities are equipped with appropriate **access control** to ensure access by authorised personnel only, including differentiation between common areas for external parties and PMB Personnel, as well as secured areas for restricted personnel. • You should also ensure that adequate **security measures** are in place such as placing security guards, CCTV, limiting access to access card holders, etc.
PMB's secure areas	• Entry to PMB's secure areas is limited to PMB's authorised personnel only as it may contain sensitive information. • PMB's secure areas may include but not limited to Traffic Monitoring Center, Record Management Centre at Seafield, etc.
Filing room	• Hardcopy information are to be maintained in an organised manner. • When accessing your BF's filing room, you should ensure that information is placed in an organised manner and a record is kept for documents and files removed from the filing room. • If you need to access information in other BF's filing room, you must obtain consent from the HOD responsible over that filing room before entering and accessing the information.

4. ACCESS CONTROL

1 PHYSICAL ACCESS

A PHYSICAL STORAGE

GENERAL

Data is also stored in equipment at various PMB's locations. If you are assigned to maintain and secure PMB's equipment for data storage, it is your responsibility to ensure that it is **kept in a secured location** taking into consideration risk of damage from fire, flood, explosion or civil unrest and other natural or man-made disasters. Further, you must also ensure that the **access** to such equipment is limited to authorised personnel only.

EQUIPMENT SECURITY:

When using such equipment, you must undertake the following security measures:

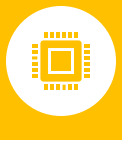
Equipment sitting & protection	• Ensure that you are authorised to have access to the equipment only for the purpose to carry out your role.
Equipment off-premises	• When you are required to use PMB's equipment outside of PMB's premises, you must ensure that **authorisation** is obtained and that the equipment is safeguarded with adequate **security features**.
Disposal or re-use of equipment	• To reuse an equipment, you must ensure that it is **overwritten** prior to reusing. • To dispose an equipment, you must ensure that it is **physically destroyed** and its content is unrecoverable.

4. ACCESS CONTROL

2 DIGITAL ACCESS

LOCATIONS WHERE DIGITAL INFORMATION IS STORED

PMB's information is also stored in various infrastructures, systems, and services as follows:

B Data Lake 	Data Lake is where data from various systems are centralised to enable different parts of PMB's business to analyse and uncover insights.
C Network 	A collection of network devices i.e. hardware, software, services, facilities or other devices connected to one another to allow sharing of data within and outside of PMB.
D Cloud 	Cloud is a virtual server running in a cloud computing via the internet and can be accessed remotely.
E Applications & Tools 	Applications & tools help integrate various data and architectures allowing business users to assess, visualise, analyse and handle data.
F End-user computing 	End-user computing refers to computer systems and platforms provided by PMB to assist you in completing your daily workload.

AREAS OF DIGITAL ACCESS

In this subsection, we will guide you on how to secure digital access in two areas as follows:

I. Access to PMB's Infrastructures, Systems and Services
II. User ID and Password Management

4. ACCESS CONTROL

I ACCESS TO PMB'S INFRASTRUCTURES, SYSTEMS AND SERVICES

WHO MAY OBTAIN ACCESS?

PMB's infrastructures, systems and services may be accessed by PMB Personnel and Authorised Third Party as follows:

1 ACCESS BY PMB PERSONNEL

To carry out your daily tasks, you may require access to information within PMB's infrastructures, systems and services. Hence, you must observe the following:

- ✓ Access may be granted by a designated HOD based on **need-to know-basis** with business justification**.**
- ✓ You must use your assigned **User ID and password** to access the infrastructures, systems or services which you have been granted approval for.
- ✓ You should only access PMB's infrastructures, systems and services using a **general account** if you have received appropriate approval from your HOD.
- ✓ HODs shall maintain and regularly review a **log of user access granted.**
- ✓ System Owners shall ensure proper **segregation of duties** to mitigate risks and possible conflicts as well as to prevent unauthorised access, fraud and errors.

2 ACCESS BY AUTHORISED THIRD PARTY ("ATP")

If you are in charge of managing an ATP who requires access to PMB's infrastructures, systems and services where information is kept, you should perform the following:

- ✓ Prior to granting access, you must ensure that a Non-Disclosure Agreement has been signed.
- ✓ Any information access required by the ATP should be substantiated with the approval of your HOD.
- ✓ Access granted to the ATP should only be up to the extend required by the ATP to fulfill their service requirements.
- ✓ All access granted must be removed once the ATP's contract has been terminated or completed.

4. ACCESS CONTROL

I ACCESS TO PMB'S INFRASTRUCTURES, SYSTEMS AND SERVICES

PRIVILEGED ACCESS

In limited circumstances, PMB Personnel or ATP may be granted with privileged access accounts such as local administrative account, privileged user account, domain administrative account, emergency account and service account. Hence, you must observe the following:

GRANTING PRIVILEGED ACCESS

- ✓ Data Owners* may grant privileged access to you based on a need-to-know basis and least privilege only.
- ✓ Data Owners* shall ensure that the usage of elevated privileges such as local and domain administrative account is minimised.
- ✓ The privileged accounts can be audited as and when required.

REVIEW, ADJUSTMENT AND REMOVAL OF ACCESS

In order to limit user access and prevent unauthorised usage of PMB's infrastructure, systems and services, you must observe the following:

REVIEW OF USER ACCESS

- ✓ Data Owners* shall review the log of **all access granted** periodically to ensure proper provision of user access, timely removal of access no longer required (due to termination or a change in employment) and efficient segregation of duties.
- ✓ If you have encountered any suspicious access, you should report the matter as an incident via the DIS Helpdesk System (DISHES).

ADJUSTMENT AND REMOVAL OF USER ACCESS

Data Owners* and DIS shall ensure the following:

- ✓ Access by **transferred** PMB Personnel have been adjusted or removed according to their new job requirement.
- ✓ Access by PMB Personnel and ATP who have **resigned, terminated or completed their contract**, is removed.
- ✓ User IDs that have been **de-activated or expired** shall not be granted to other individuals.

* Data Owners refer to HODs who manage information under their purview.

4. ACCESS CONTROL

II USER ID AND PASSWORD MANAGEMENT

GENERAL

As PMB moves towards information digitisation, it is crucial for you to ensure sufficient security measures are in place to protect the security of information in your IT devices and while using PMB's IT infrastructures, systems and services.

In this section, we will guide you on how to set, protect and manage your **User ID** and **password.** Here are some tips for your user ID and password:

HOW TO SET YOUR USER ID?

As a PMB Personnel, you will be **assigned a company's User ID** by DIS i.e. the username from your official email account.

HOW TO SET YOUR PASSWORD?

After your User ID is set, it is important for you to 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 are **inactive** on your end-user computing system for more than 30 minutes, you may have to re-enter your User ID and password for authentication.
- If you attempt to insert the **wrong password** for 3 times, 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 your password is suspected to be compromised, you should report to DIS and change all relevant passwords.

4. ACCESS CONTROL

II USER ID AND PASSWORD MANAGEMENT

HOW TO MANAGE YOUR USER ID AND PASSWORD?

Upon setting your User ID and password, you must protect them to avoid unauthorised access to your PMB accounts by considering the following:

- ✓ You should only use your designated User ID when logging into any PMB's system.
- ✓ You should **change your password** every 75 days.
- ✓ You should not use any of your 15 **previous passwords.**
- ✓ You should not **write down or store** your passwords digitally in an unsecured environment.
- ✓ You should **use different password** for PMB accounts from other non-PMB related accounts and refrain from using username as your password.
- ✓ You should keep your password safe and private as you will be held responsible for all activities done using your User ID. You must **avoid from revealing, displaying, talking or even hinting** about your password to other people or in any forms.

- ✗ DO NOT use a User ID that is not designated to you when logging into any PMB's system.
- ✗ DO NOT set a **weak password** for your user account.
- ✗ DO NOT use **group accounts, shared passwords** or other authentication methods unless special approval is obtained with business justification.
- ✗ DO NOT **share your PMB related account passwords** with anyone (including superiors, IT administrators or family members) in any e-mail, text message or verbally over the phone. All passwords are to be treated as PMB's sensitive and confidential information.
- ✗ DO NOT use the **"Remember Password"** feature of applications (e.g., Outlook, Proxy).

4. ACCESS CONTROL

SCENARIOS

1.

Q Your colleague has retrieved a "Highly Confidential" document from the filing room without updating the logbook. You discover that the document is missing. What should you do?

A ***You should check with your colleague and remind them to always update the logbook. If the document cannot be found, you should inform your HOD and report to C&I on the incident immediately.***

2.

Q A vendor is appointed to upgrade the equipment in the server room. What should you do to ensure the security of the equipment?

A ***You should obtain your HOD's approval for the vendor representative to access the server room. While the vendor representative is working in the server room, you should monitor him/her to ensure there is no damage, pilferage or any suspicious act.***

3.

Q You are granted with access to the Oracle system. One day, your colleague who also has access to the Oracle System is facing technical issues with her Oracle account. She has requested for you to share your User ID and password as she needs to post a transaction urgently. Can you share your account with your colleague?

A ***No, you should maintain confidentiality of your User ID and password as you are accountable for the information security of PMB's system.***

4.

Q You are tasked to lead a special project which requires access to Data Lake. What should you do to ensure the security of the information stored in Data Lake?

A ***You should discuss with your HOD on the need to access Data Lake and obtain approval from the System Owner. The access granted to you should not be shared with anyone else.***

5.

Q You have appointed a consultant to enhance the CCOMS application and the consultant requires access to the application. What should you do before granting access?

A ***You should understand the purpose and extend of access required by the consultant, followed by ensuring a Non-Disclosure Agreement or contract with confidentiality clause has been executed. Approval from your HOD should be attained prior to granting access and access must be revoke upon completion of the project.***

6.

Q You are a new joiner and you have collected your PMB issued laptop from DIS. You were given a User ID and temporary password. What should your immediate action be?

A ***You should immediately change the password. It is pertinent for you to set a strong password based on recommendation on page 36 of this ISPG 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.

5. INFORMATION SHARING

GENERAL

In carrying out your daily tasks, you may be required to share information internally and externally with various 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. Within PMB
   - B. Public Communication
   - C. Regulators & Government Bodies
   - D. Other external request for PMB's information
2. Specific examples and guidelines for sharing information through messaging application and social media
   - A. Messaging Applications
   - B. PMB's Social Media
   - C. Personal Social Media

5. INFORMATION SHARING

1 SHARING OF INFORMATION INTERNALLY AND EXTERNALLY TO VARIOUS PARTIES VIA FORMAL AND INFORMAL MECHANISM

OVERVIEW OF INTERNAL & EXTERNAL INFORMATION SHARING

This section guides you on how to share information in a secured manner internally and externally on various platforms. The following provides an overview of the areas covered under this section:

A Within PMB 	How do you ensure information shared within your business function or across business functions is secured.
B Public Communication 	What are the precautions, considerations and security measures you need to undertake prior to sharing information to the public.
C Regulators & Government Bodies 	How do you ensure information shared (e.g. project update, traffic data, etc.) with regulators or Government bodies are secured.
D Other external request for PMB's information 	How do you ensure information shared with other external parties is secured. This may include instances where you may be required to respond to requests, queries, complaints or fulfilling any contractual obligations.

5. INFORMATION SHARING

A WITHIN PMB

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Written
- Email
- Letter
- Form
- Memo
- Internal systems such as PLUSLounge, Sharepoint, etc.

Verbal
- Meeting
- Call

Before sharing information, you must **consider** the following:

- ✓ Is the information **relevant and accurate**?
- ✓ What is the **purpose** of sharing the information?
- ✓ Who is the **intended audience and** how will the information be used?
- ✓ Whether information to be shared is a **finalised version** or a **working draft**?
- ✓ Have you obtained the **relevant approval** to share information?
- ✓ How to share **"Highly Confidential", "Restricted" and "Internal"** information?
- ✓ What is the **proper platform** for work discussion?

Do's
you SHOULD

- ✓ You should ensure that the information shared is **relevant and accurate**.
- ✓ You must be aware of how the information will be used by the intended audience.
- ✓ Whenever possible, you should share **finalised information in uneditable version**. However, if it is necessary for you to share a working draft, , you are encouraged to **watermark it as "draft".**
- ✓ You should ensure relevant **approval** is obtained in-line with information classification.
- ✓ When sharing **"Highly Confidential" information,** you must label the document with its information classification and encouraged to include confidentiality statement.* You are encouraged to do the same for **"Restricted"** and **"Internal"** information.
- ✓ Whenever possible, you should discuss using **official written platform** such as email. However, if it is necessary to discuss over messaging application such as WhatsApp, you are encouraged to follow up with an official email.

Don'ts
you SHOULD NOT

- × DO NOT share **outdated** and **inaccurate** information.
- × DO NOT share **more than** the information requested.
- × DO NOT share the information beyond the intended audience.
- × DO NOT share the information received from other BF **without proper approval** from the HOD.
- × DO NOT share **"Highly Confidential"** information without labelling the document with its information classification*
- × DO NOT transfer any PMB's information using **removable storage devices** such as thumb drives and hard disk unless you are authorised and records of the transfer is kept.

**Note: Please refer to "Information Classification" and "Information Handling and Labelling" section for further explanation on information classification and confidentiality statement.*

5. INFORMATION SHARING

B PUBLIC COMMUNICATION

RISK & APPROVAL

Under certain circumstances, PMB may need to communicate PMB's information to the public via various platforms including the media, PLUS corporate websites and applications. This may involve "Public" information with different levels of risk and approval requirements as follows:

Low risk	Information is **consulted** and **approved** by **HOD.**
High risk	Information is **channelled through CC, reviewed by relevant C-Suites and approved by MD**.

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Written & Verbal:
- Media release
- Interview
- Customer survey/ Newsletters
- Spokesperson speeches
- Feature stories
- FAQs
- eBooks on PLUS related projects

PMB's channel:
- PLUS website
- PLUSMiles website
- PLUS App

Before sharing information, you must **consider** the following:

- ✓ Is the information **verified** and from a **reputable source**?
- ✓ Is the information **relevant and accurate**?
- ✓ What is the **purpose of sharing the information to the public?**
- ✓ Who is the intended **target audience**?
- ✓ Whether information to be shared is a **finalised version** or a **working draft**?
- ✓ Whether the information is written in the proper **tone** and **language** commonly used by PMB?
- ✓ Is it necessary to undertake any measures to **mitigate the impact of information publication**, including the inclusion of a disclaimer?
- ✓ Whether sharing the information may **stir controversy**?
- ✓ Will there be any **financial or reputational impact** in result of the communication?
- ✓ Have you obtained the **relevant approval?**
- ✓ Have you obtained the relevant approval internally aligned to the risk level above?
- ✓ Are you the designated personnel who is authorised to share the information to the **media** or to post on **PMB's channels**?
- ✓ What is the **suitable time** to release information?

Refer to page 43 for do's and don'ts for public communication.

5. INFORMATION SHARING

B PUBLIC COMMUNICATION

Do's
you SHOULD

- ✓ You should ensure that the information is verified and from a reputable source.
- ✓ You should ensure that the information to be shared is **relevant and accurate.**
- ✓ You should understand the **purpose** of information sharing to the public.
- ✓ You should determine the **target audience.**
- ✓ You should always share **finalised information in uneditable version**. However, if it is necessary for you to share a working draft, you are encouraged to **watermark it as "draft"** and include a disclaimer that the draft information should not be published until it is finalised.
- ✓ While preparing the information to be published, you should ensure that the **tone and language** used is in line with PMB's common writing style.
- ✓ Whenever necessary, you should undertake relevant **measures to mitigate** the impact of information publication such inserting a disclaimer.
- ✓ You should assess the information to be shared from various angles to avoid **controversy**.
- ✓ You should consider the **risk of financial and reputational impact** when preparing the information for publication.
- ✓ You should obtain the relevant **approva**l to publish the information in line with its **risk level**.
- ✓ You must be **authorised by your HOD** to share information to the media or to post on PMB's channel.

Don'ts
you SHOULD NOT

- × If a **third party's information, name or logo** is inserted in a public statement, DO NOT release the statement without obtaining **third party's written consent**.
- × DO NOT share information without obtaining the **relevant approval to publish the information** in line with its risk level.
- × DO NOT share information with the media or post on PMB's official channel **without authorisation** from your HOD.

5. INFORMATION SHARING

C REGULATORS & GOVERNMENT BODIES

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Written
- Email
- Letter
- Form
- Official website

Verbal
- Meeting
- Call

Before sharing information, you must **consider** the following:
- ✓ Is the information relevant **and accurate**?
- ✓ What is the intended **usage of** information shared?
- ✓ Are you **sharing more** than what is required with the regulators?
- ✓ Do you need to **label the document** with its information classification and insert **confidentiality statement**?
- ✓ Whether information to be shared is a **finalised version** or a **working draft**?
- ✓ If there is any third party information involved, have you obtained the third **party consent**?
- ✓ Have you obtained the **relevant approval?**
- ✓ Are you using the **secured and formal platform** to share information?

Do's
you SHOULD

- ✓ You should ensure information to be shared is **relevant and accurate.**
- ✓ You must enquire on how the information will be used.
- ✓ When sharing "Highly Confidential" information, you should ensure that the document is labelled with its information classification and inserted confidentiality statement. You are highly encouraged to do the same before sharing "Restricted" information.
- ✓ You should always share **finalised information in uneditable version**. However, if it is necessary for you to share a working draft, you are encouraged to **watermark it as "draft".**
- ✓ You should obtain relevant **approval** in-line with information classification.

Don'ts
you SHOULD NOT

- × DO NOT share information **beyond** what is requested.
- × DO NOT share information without obtaining the relevant **approval.**
- × DO NOT use **unsecured and informal platform** to share information.

5. INFORMATION SHARING

D OTHER EXTERNAL REQUEST FOR PMB'S INFORMATION

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Written
- Email
- Letter

Verbal
- Meeting
- Call

Before sharing information, you must **consider** the following:
- ✓ Is the information **relevant and accurate**?
- ✓ What is the **purpose** of sharing the information?
- ✓ Are you **sharing more** than what is requested?
- ✓ Do you need to **label the document** with its information classification and insert **confidentiality statement**?
- ✓ Will there be any **financial or reputational impact** in result of the information sharing?
- ✓ Is it necessary to undertake any measures to **mitigate the impact information sharing**, including the inclusion of a disclaimer?
- ✓ Whether the sharing involves any third party's information. If yes, it is necessary to obtain third **party consent**?
- ✓ Have you obtained the **relevant approval** to share information?
- ✓ Whether it is necessary for external party to sign a **Non-Disclosure Agreement**?
- ✓ What is the **proper document format** to share information?
- ✓ Are you using the **secured and formal platform** to share information?

Do's
you SHOULD

- ✓ You should ensure that the information to be shared is **relevant and accurate**.
- ✓ You should consider the **risk of financial and reputational impact** before sharing information.
- ✓ You must enquire on how the information will be used.
- ✓ When sharing "Highly Confidential" information, you should ensure that the document is labelled with its **information classification** and you are encouraged to include **confidentiality statement**. You are highly encouraged to do the same before sharing "Restricted" information.
- ✓ Whenever necessary, you should undertake relevant **measures to mitigate** the impact of information sharing such as inserting a disclaimer.
- ✓ You should obtain relevant **approval**.
- ✓ You should ensure the information is shared using the **secured and formal platform**.

Don'ts
you SHOULD NOT

- × DO NOT share **outdated and inaccurate** information.
- × DO NOT share information prior to external party signing a Non-Disclosure Agreement.
- × If a **third party's information, name or logo** is involved, DO NOT share without obtaining third party's consent.
- × DO NOT share information **beyond** what is requested.
- × DO NOT share information without obtaining the relevant **approval.**
- × DO NOT share **finalised information in editable format.**

5. INFORMATION SHARING

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

OVERVIEW OF INFORMATION SHARING THROUGH MESSAGING APPLICATION AND SOCIAL MEDIA

This section guides you on how to share information in a secured manner using messaging applications and social media. The following provides an overview of the areas covered under this section:

A **Messaging Applications**

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.

What are the considerations and precautions you need to undertake when sharing PMB's information across messaging applications?

B **PMB's Social Media**

In instances where you are tasked to post PMB's official information and announcement, you may be required to use PMB's official social media channels.

What are the considerations and precautions you need to undertake when sharing PMB's information using PMB's official social media?

C **Personal Social Media**

It is important for you to remember that your actions and interactions on social media may be affiliated with PMB. Hence, you need to ensure that you take precautions when using your social media wisely as to protect the organisation's interest as well as yourself from disciplinary action.

What are the considerations and precautions you need to undertake when sharing PMB's information or any information that may be associated to PMB using your personal social media?

5. INFORMATION SHARING

A MESSAGING APPLICATIONS

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Messaging applications (written & verbal)
- WhatsApp
- Telegram
- WeChat
- Line
- Google Hangouts
- Facebook Messenger
- Viber etc.

Before communicating and sharing (e.g. texting, sharing documents, pictures or videos) any information that may have association with PMB, you must **consider** the following:

- ✓ What is the **purpose** of sharing the information?
- ✓ Who is the **intended recipient?**
- ✓ Do you need to **label the document** with its information classification and insert **confidentiality statement**?
- ✓ Whether information to be shared is a **finalised version** or a **working draft**?
- ✓ Will there be any **reputational impact** as a result of an information sharing?
- ✓ Whether is it appropriate for you to share information/ conversation from a WhatsApp message/ **WhatsApp group chat** to others in any form?
- ✓ Prior to sharing information to a group chat, determine whether the members of the group chat are required to receive the information?
- ✓ Have you sought permission from the sender prior to **forwarding any message** that you received?

Do's
you SHOULD

- ✓ You should understand the **purpose** of sharing the information.
- ✓ You should consider the **risk of reputational impact** before sharing information.
- ✓ You should send to the message to the right **recipient only**.
- ✓ When sharing "Highly Confidential" documents, ensure they are labelled.
- ✓ You should share **finalised information in uneditable version**. However, if it is necessary for you to share a working draft, you are encouraged to **watermark it as "draft"**.
- ✓ 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.
- ✓ If you had a work discussion via a messaging application, you are encouraged to **follow up with an email** to confirm the details of the discussion.

Don'ts
you SHOULD NOT

- × DO NOT share PMB's information **without authorisation**.
- × DO NOT allow other people to access your work-related messaging group chats.
- × DO NOT share work related information from a **group chat** to other people who are not within the WhatsApp group.
- × DO NOT **forward any message** you received or screenshot of a message without the permission of the sender.
- × Avoid sharing pictures or videos which may be controversial e.g. picture of an injured customer in an accident, not wearing face mask when required etc.

5. INFORMATION SHARING

B PMB'S SOCIAL MEDIA*

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

PMB's social media accounts:
- Facebook
- Twitter
- Instagram
- LinkedIn
- Youtube etc.

Before sharing information, you must **consider** the following:
- ✓ Is the information **verified** and from a **reputable source**?
- ✓ Is the information **relevant and accurate**?
- ✓ What is the **purpose** of sharing off information?
- ✓ Who is the **intended recipient?**
- ✓ What are the precautions you should undertake before sharing any **PMB's news or announcements**?
- ✓ Will there be any **financial or reputational impact** in result of the online posting?
- ✓ Do you need to undertake any measures to **mitigate the impact of information sharing**, including the inclusion of a disclaimer?
- ✓ Whether it is necessary to obtain **third party consent**?
- ✓ Are you the designated personnel authorised to post PMB's information **using PMB's official social media account**?
- ✓ Have you obtained the **relevant approval** to share information?
- ✓ Which **social media account** is suitable to post on behalf of PMB online?
- ✓ What is the **suitable time** to release information?

Do's
you SHOULD

- ✓ You should understand the **purpose** of information sharing to the public.
- ✓ You should consider the **risk of financial and reputational impact** before sharing information.
- ✓ You should determine the **target audience.**
- ✓ You must seek authorisation from **your HOD** to share information to the media or to post on PMB's channel.
- ✓ You should obtain relevant **approval**** in-line with information classification.
- ✓ You should ensure that **any news or announcements** about PMB should come from a trusted official media or source before sharing.
- ✓ Whenever necessary, you should undertake relevant **measures to mitigate** the impact of information sharing such as inserting a disclaimer.
- ✓ When posting on behalf of PMB, ensure to **use PMB's official social media**.

Don'ts
you SHOULD NOT

- × DO NOT delegate your responsibility to post PMB's information **using PMB's official social media account** in your absence without your HOD's approval.
- × If a **third party's information, name or logo** is involved, DO NOT share the information without obtaining third party's written consent.

Note:
** As sharing information in social media is a form of public communication, please refer page 42 on considerations and precautions for "Public Communication" as the same are applicable to this subsection.*
***For routine information sharing using PMB's social media, HOD may delegate or give blanket approval to you to carry out your daily duties to publish low risk "public" information on PMB's social media.*

5. INFORMATION SHARING

C PERSONAL SOCIAL MEDIA

PLATFORM OF COMMUNICATION & CONSIDERATION

Information may be shared via the following **platforms**:

Online blogs, forums, messaging sites and social media websites including:

- Facebook
- Twitter
- Instagram
- TikTok
- LinkedIn,
- Youtube etc.

Before interacting online (e.g. sharing, posting, forwarding, liking or reacting) to any articles, written posts, pictures, videos etc. involving any information that may have association with PMB, you must **consider** the following:

- ✓ Is it from a verified, reputable or official source?
- ✓ Have you obtained approval from your HOD to use **PMB's name or logo** to represent any initiative, programme, non-profit organisation, etc.?
- ✓ Is it appropriate and will it cause any **reputational impact to PMB or result in any misconduct**?
- ✓ Have you included a **disclaimer** that any views shared in your social media are personal and do not reflect the stance of the organisation?

Do's
you SHOULD

- ✓ When sharing PMB related information, please ensure that it is from a verified, reputable or official source.
- ✓ You should always consider the **reputational impact** as a result of your interaction.
- ✓ Refrain from **replying to online comments** that is damaging to PMB's reputation and report to CC for further action.
- ✓ When sharing **pictures/ videos** while working, please ensure that there is no sensitive information in the picture/ video.
- ✓ When sharing **pictures/ videos** while working, avoid any controversy that may arise as a result of the sharing.
- ✓ Discuss with your HOD or use PMB's official whistleblowing channel if you have work related concerns about your **colleagues, superiors, subordinates, customers, vendors, business partners and any other parties who are engaging with PMB** rather than posting on your personal social media.

Don'ts
you SHOULD NOT

- × DO NOT share PMB related information that is not from a verified, reputable or official source.
- × DO NOT use PMB's name and logo to represent any initiative, programme, non-profit organisation, etc. **without PMB's written approval**.
- × DO NOT share PMB's information categorised as "Internal", "Restricted" and "Highly Confidential" and has **not been released by PMB publicly**.
- × DO NOT post any pictures/ videos taken with visible **non-public PMB's information**.

Note: As a PMB Personnel, you are expected to carry yourself as per required under the Code of Conduct. Be mindful that your actions may be affiliated with PMB. You are also encouraged to put a disclaimer on your social media account to indicate that your views and opinions do not the reflect the stance of the organisation.

5. INFORMATION SHARING

SCENARIOS

1.

Q You are developing a policy for PMB which requires input from other BFs. Can you share the draft policy with other BFs?

A ***Yes, you may share the information with other BFs upon obtaining your HOD's approval. As the policy has not been finalised, you are encouraged to insert "DRAFT" watermark in the document.***

2.

Q Your colleague from Toll BF has asked you to share a document that you recently acquired from Real Estate BF. Can you share the document with your colleague?

A ***No, you should not share the document that you acquired from other BF. You should refer your colleague to request from that BF directly or you may seek approval on his/her behalf.***

3.

Q PMB is nominated for the Best Highway Operator award and is invited to attend award ceremony next Monday. Thus, you are tasked to prepare a public release on this award. What should you do to ensure timely announcement of press release on PLUS website?

A ***You should draft the press release and obtain approval in advance. If PMB is announced as the award winner during the ceremony, you should publish the press release and the photo taken during the ceremony immediately or suitable time advised by CC to share PMB's achievement to the public.***

4.

Q There was a technological breakthrough on your RFID project and you were approached by a radio station for an interview. What should you do?

A ***Firstly, you should find out more about the interview, such as the objective, scope and audience. Following that, you should channel the request through CC as guided by page 42 of this ISPG.***

5.

Q You have launched an e-Book about RFID on PLUS website. Subsequently, a reporter approaches you to obtain information on RFID. Can you share the information with the reporter?

A ***You can share information that is publicly available on PLUS website to the reporter. However, you should obtain approval as stated on page 17 of this ISPG before sharing any non "Public" information.***

6.

Q MHA has verbally requested for a detailed explanation on a flooding incident that happened recently. As the Region Manager, how should you respond to such request?

A ***You should respond officially to MHA via a formal written communication such as letter or report with relevant confidentiality statement and label based on information classification.***

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

5. INFORMATION SHARING

SCENARIOS

7.

Q A postgraduate has requested for traffic data to complete his research study. Can you share the information requested?

A ***Yes, you can share the information after performing the following:***

- ***Understand how PMB's information will be used;***
- ***Check the validity of the request (e.g. supporting letter from university);***
- ***Obtain approval based on information classification; and***
- ***Execute a Non-Disclosure Agreement or any other agreement with confidentiality clause with the Requestor.***

8.

Q You have received a file from Toll group chat which you find that it relevant for Enterprise Risk. Can you share the file with your Enterprise Risk group chat?

A ***No, the members in Enterprise Risk group chat may not be the intended audience for the file shared in Toll group chat. You should seek permission from Toll before sharing the information.***

9.

Q Your friend sent you a forwarded WhatsApp message on toll discount for Penang bridge during Hari Raya festive season. As you are excited with the news, can you spread the news?

A ***As a PMB Personnel, you should verify the accuracy of the information related to PMB prior to sharing. By sharing inaccurate information about PMB, you may be subject to disciplinary action for spreading rumours/ fake news.***

10.

Q Your HOD has communicated to you via WhatsApp to revise the work arrangement of the contractor under your care. To simplify communication with the contractor, can you forward the screenshot of your conversation with your HOD to the contractor?

A ***No, you should inform your contractor on the outcome of your discussion rather than to send the screenshot of your conversation with your HOD. This is to prevent any leakage of internal discussion which is not meant to be shared to the contractor.***

11.

Q You saw an interesting footage captured by PMB's CCTV. Can you share it with your friends and family?

A ***No, PMB's CCTV record is non "Public" information. You should not share it without authorisation as you may not be fully aware of the potential impact on PMB's reputation.***

12.

Q You have created a WhatsApp group chat for a team comprising of PMB Personnel, consultants and contractor to discuss on a renovation project. A decision was made via the group chat. What should you do to secure this decision?

A ***As the messages in the group chat may not be read or saved by the recipients, you should send an email to relevant recipients to summarise the outcome of the discussion in the group chat.***

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.

5. INFORMATION SHARING

SCENARIOS

13.

Q While patrolling on PLUS highway, you encountered a car accident. Can you take a photo of the accident and send it to your family as warning of possible traffic jam?

A ***As a PMB Personnel, it is highly encouraged for you to refrain from sending photo of the car accident to any third party to prevent any misinterpretation or misuse of photo that you shared. You may inform your family directly without providing picture or video of the accident.***

14.

Q As a Customer Experience Management Executive, you have recently been tasked to post accident update on PLUS App routinely to warn highway users on the accident along the highway. Are you required to obtain approval before each posting?

A ***As this is a routine posting, your HOD may provide you with a blanket approval which authorises you to post accident update as and when required.***

15.

Q You are designated by your HOD to manage PMB's LinkedIn account. As you are on leave today, can you share your User ID and password to your colleague who will assist you in managing PMB's LinkedIn account when you are away?

A ***No, you should not delegate your responsibility to post PMB's information using PMB's official social media account in your absence without your HOD's approval.***

16.

Q PMB has signed a Memorandum of Understanding with a Business Partner to collaborate on a project. As you would like to share this positive news on PMB's social media, what should you do?

A ***Firstly, you should consider guidance on page 42 of this ISPG and check the Memorandum of Understanding or any other agreement to understand PMB's obligation in relation to confidentiality. You should also obtain consent from your Business Partner and speak to CC for the next course of action.***

17.

Q You noticed a negative review on Facebook regarding poor upkeep and bad service at PMB's Rest and Service Area. What should you do?

A ***You should refrain from responding to that post to avoid any complication/ antagonisation. You should inform CC immediately to address the situation.***

18.

Q Upon approval to launch PMB's Sustainability report, you as the administrator of PMB's social media account are tasked to post this announcement on PMB's Facebook and LinkedIn. Can you post it concurrently on your personal social media?

A ***No, you should post it on PMB's Facebook and LinkedIn only. Once the announcement is made public, you can then proceed to share the post from PMB's social media on your personal social media account.***

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.

5. INFORMATION SHARING

SCENARIOS

19.

Q You have taken photos with your colleagues during PMB's Integrity Day. Can you post the photos on your personal social media?

A ***In general, you may post photos about a PMB's event on your personal social media. However, you must be mindful of the content being posted to prevent any controversy, e.g. PMB Personnel not wearing a face mask during the event which is a violation of the Standard Operating Procedure issued by the Government during Covid-19 pandemic.***

20.

Q You have initiated a personal donation drive to help fence-line community impacted by the recent flash flood. Can you use PMB's name and logo to promote this donation drive?

A ***No, you should not use PMB name and logo for any event/ activity that is not officially organised by PMB. You should indicate that the donation drive is your own personal initiative.***

21.

Q You were upset that you did not receive a promotion and you would like to vent your frustration that your superior had broken his promise on your personal Facebook. Can you post such posting?

A ***No, social media is not a proper channel to express or resolve your work-related concerns and issues. You should always refer to the relevant channel within PMB to assist you on work-related issues such as your HOD, HRR and Speak Up Channel.***

22.

Q You are grateful with the opportunity given by PMB to work from home. Thus, you would like to take a selfie featuring you and PMB issued laptop at home and post it on your personal Instagram. Can you do so?

A ***Yes, you can post the selfie. However, prior to posting the picture on your Instagram, you should ensure that no sensitive PMB's information is captured on the laptop screen and surrounding. This is to prevent leakage of PMB's information.***

23.

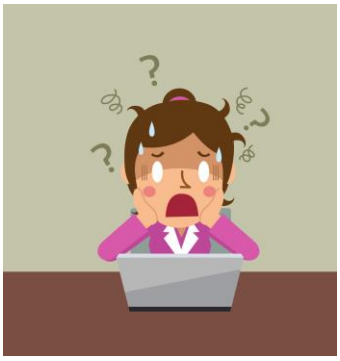
Q As a Management Executive of Sustainability, you are inclined to post on your Facebook to express your viewpoint in relation to forest de-gazettement. What should you do to protect your personal and PMB's interest?

A ***You should be mindful that public may perceive your action and viewpoint to be affiliated with PMB. To protect your personal and PMB's interest, you should include a disclaimer in your posting to indicate that this is your personal viewpoint and does not represent PMB.***

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.

5. INFORMATION SHARING

WHAT IS THE IMPACT OF UNAUTHORISED INFORMATION SHARING?



If you share information without proper approval, you may be at risk at causing the following:

- Damage PMB's **reputation, competitive advantage and financial prospects**.
- If the information is provided pursuant to any agreements which require a third party approval, failure to get the third party approval before sharing information may put PMB at risk of facing **legal suits**.
- If a **customer's personal information** is being shared without authorisation, PMB and PMB Personnel involved may be at risk of being sued, compounded or imprisoned if proven guilty for breaching the Personal Data Protection Act 2010.
- **Disciplinary action** may be taken against you for breaching this ISPG.

WHAT TO DO IF YOU HAVE DOUBTS ABOUT INFORMATION SHARING?

If you have any doubts or require any clarification before sharing PMB's information on any platform to any party, please reach out to your **HOD** or **C&I** to confirm on the matter and the necessary approval to be obtained before sharing PMB's information.

WE ARE HERE FOR YOU

QUERIES AND INCIDENT REPORTS

How can we help you?

Describe your issue

You should always feel free to discuss questions regarding this ISPG with your Manager, HOD, DIS, Cybersecurity or C&I.

However, should you require further clarification on this ISPG or to report on any information security breach incidents that is non-technical and unrelated to cybersecurity, please contact C&I at compliance@plus.com.my or directly contact any C&I team members.

If you would like to report on any information security breach incidents that is technical in nature and related to cybersecurity, please contact DIS via DIS Helpdesk System (DISHES), email at helpdesk.dis@plus.com.my, Microsoft Teams (Digital Initiative Studio Helpdesk) or via phone call at 03-7666 4041/ 4048.

PMB reserves the right to amend this ISPG at any time