MALAYSIA RAIL LINK

Acceptance of IT Equipment

ACCEPTANCE OF IT EQUIPMENT

By signing this document, the recipient of the IT equipment agrees to be fully responsible for ensuring that the equipment is adequately maintained, and the safety of the equipment and the data stored in it is ensured. Any negligence made by the Recipient over the Equipment is the Recipient's sole responsibility.

In the event of loss or damage to equipment, a report must be made through IT ServiceDesk for action. In the event of loss and damage, the company has the right to enforce its policies and procedures, including paying back the equipment or the repair cost.

Equipment Recipients have also understood the MRLSB IT Security Policy and the statement at the back of this form.

A. STAFF DETAIL

1.	Staff Name	: NUR SYAM MAHIRAH BINTI JILAH	Staff No.	: MRL00455
2.	Designation	: DOCUMENT CONTROLLER	Location (HQ / SITE)	: SECTION 8

B. EQUIPMENT DETAIL

Equipment Type:	NOTEBOOK (HP ProBook 440 G5)	**Serial No.**	5CD825029H	**Asset Tag:**	MRL00005091

No.	Item / Accessories	Quantity	Acceptance	Return *
1.	USB Optical Mouse (Wired)	1	☑	□
2.	AC Adapter & Power Cable	1	☑	□
3.	Docking & Power Cable		□	□
4.	USB Keyboard		□	□
5.	Backpack	1	☑	□
6.	Other:			
	(a) Adapter for LAN & VGA		□	□
	(b)		□	□
	(c)		□	□
	(d)		□	□

*** *Reviewed when staff end of service or change of new equipment. End of Service shall be attached with HR Exit Form***

C. ACCEPTANCE AND VERIFICATION

Handover by (IT Department):	**Acceptance of Equipment by:**	**Verification of Acceptance (IT Manager)**
Name: MUHAMMAD SYAIRAZI BIN SHAHARUD Designation: IT PESONNEL Date: 21/11/2024	Name: NUR SYAM MAHIRAH BINTI JILAH Designation: DOCUMENT CONTROLLER Date: 21/11/2024	Name: Designation: Date:

D. RETURN OF EQUIPMENT

Received by (IT Department):	**Return of Equipment by:**	**Verification of Return Equipment (IT Manager)**
Name: Designation: Date:	Name: Designation: Date:	Name: Designation: Date:

Acceptance of IT Equipment

BRIEF OF IT SECURITY POLICY AND IMPORTANT NOTICE TO USER

Use of Computers
Users will be provided with Information Technology and Systems facilities to help them carry out the tasks required of them. Users should adhere to the following directives when utilizing these facilities:

I. Mobile Computing & Other IT Devices
Mobile computing devices such as laptops and other smart devices have become useful tools to meet the business need. Such devices are particularly susceptible to loss, theft and hacking as they are easily portable and can be used anywhere outside of the MRLSB's network.

The purpose of this policy is to establish the rules for the use of mobile computing devices that contain or access information resources at the MRLSB. It is crucial to preserve the confidentiality, integrity, and availability of the MRLSB's information.
(a) Data Repository and Backup

- *Users are advised to keep to a minimum the amount of confidential, personal, or sensitive MRLSB information stored on the computer's hard drive or any smart devices.*
- *Users are responsible for ensuring all the work-related data stored on computers or any smart devices is regularly backed up or synchronized to OneDrive.*
- *Users are to perform housekeeping on their OneDrive file storage to ensure it does not exceed storage quota limit*
- *Usage of removeable media devices (such as thumb-drive, external Hard-drive will be restricted*

(b) Software Installations and Configurations

- *Users are not authorized to install any software or change the configuration of the MRLSB provided mobile computing devices.*
- *Any installation or change of configurations will require ITD's review and approval. The request for any change must be sent to the IT ServiceDesk.*

(c) Personal Use

- *Users should not use the MRLSB provided mobile computing or IT devices for personal use (any purpose not specifically related to the MRLSB work).*
- *Users should only use the MRLSB provided IT device to access systems and services for which they have been authorized.*

(d) Usage by a Third-party/Vendor

- *Users are responsible for ensuring that any use of the MRLSB provided mobile computing or IT devices by a third party is consistent with this Policy.*

(e) Physical Security

- *Users are responsible for the physical security of the MRLSB owned mobile computing and IT devices assigned to them.*
- *MRLSB provided mobile computing and IT devices must not be left unattended. The devices should be locked or kept in a secured area or place when not in use.*
- *In any event of theft, loss or compromised of any MRLSB's mobile computing equipment or IT devices, they must:*
  - *Lodge a Police immediately*
  - *Inform ITD in-writing about the event/case/incident immediately.*
  - *In case of faulty, user must lodge report at IT ServiceDesk.*

II. Access and Password
(a) Access Management

- *All Access Management shall adherence MRLSB Access Management Policy.*
- *All users who require access to system and information resources are properly identified by means of a unique personal identifier and password.*
- *Access levels to systems/applications are granted as per defined in the Service Request approved by user's respective superior.*
- *Users are responsible for all computer access transactions that are made with his/her user ID and password.*

(b) Password Management

- *All Password Management shall adherence MRLSB Access Management Policy.*
- *Users are required to change their system login password every 90 days.*
- *Passwords must be of a minimum of 8 characters long and contain at least one capital letter and alpha numeric character.*
- *Users must not disclose passwords to others. For multi-user mailboxes, users must not disclose the password to any unauthorized personnel.*
- *Do not attempt to access the accounts of other individuals.*
- *Users must change their password immediately if it is suspected that it has become known to another individual.*
- *Users are advised to avoid using the same password on multiple accounts.*

Access to IT Security Policy is via MRLSB's Internal Portal

MALAYSIA RAIL LINK

Installation Checklist

INSTALLATION CHECKLIST

A. HARDWARE DETAIL

1.	Computer Name	: MYCDS8-HAZ	Username	: haznurul.ain
2.	Staff Name	: NUR SYAM MAHIRAH BINTI JILAH	Staff No.	: MRL00455

B. BEFORE DELIVERY – EQUIPMENT PREPARATION

I. Domain Configuration

1. Create Computer Name	☑	2. Enable Administration account	☑	3. Set Admin Password	☑
4. Turn off User Account Control	☑	5. Join Domain	☑	6. Create User Profile	☑

II. Software Installation & Standard Configuration

1. Office & Outlook	☑	2. Mozilla & Chrome	☑	3. Manufacturer Support Assistance	☑
4. Adobe Reader	☑	5. Archive Software (Zip)	☑	6. Antivirus Software	☑
7. Printer Driver & Default of Printer	☑	8. Scan & Shared Folder	☑	9. Turn off Firewall	☑
10. Word – set A4 size & show ruler	☑	11. Clean the Desktop	☑	12. PIN Office Apps to Taskbar	☑
13. Configure Virtual Private Network	□	14. Clear All Icon from Start Menu	☑		□

Other Installation & Configuration. Only for not standard item (please note)

	□		□		□
	□		□		□

III. EQUIPMENT ACCEPTANCE & USER BRIEFING

1. Change User Password	☑	2. Access of O365 Apps (Email etc)	☑	3. Shared Folder	☑
4. Sync User's One Drive	☑	5. Signed Acceptance Form	☑	6. Understand of User Responsibility	☑
7. Inform on Password Policy	☑		□		□

IV. AFTER DELIVERY: DATA ENTRY & ASSET RECORD

1. Stored Acceptance Form in IT SharePoint for verification.	☑	2. Update the Asset Record in IT Asset / AMS	□
	□	• Detail info of the Asset (Key-in all the related field)	□

C. COMPLETION OF TASK

Configured by (IT Technician) Syairazi Name: MUHAMMAD SYAIRAZI BIN SHAHARUDIN Date: 20/11/2024	**Verified by (IT Manager):** Name: Date: