User ID Issuance and Termination

1. Introduction

Access to MTD's information systems is controlled by each user assigned with a user id and having the accounts created to access various computing resources such as Microsoft Windows and email as required.

2. Objective

The objective of this document is to define a set of guidelines for defining and maintenance of user ids within the organization.

3. Scope

This policy applies to all staff including temporary users such as vendors, contractors and consultants accessing and using networked systems through any facility of the company. Such resources include computer and network systems, hardware, databases, support services, physical facilities, data communication systems and services.

4. Definitions

User

A user is a person who uses MTD's information systems or connect their own system into the network including systems that do not require user authentication.

System Administrators (HQ)

System Administrators are responsible for monitoring, maintaining security systems, implementing procedures to protect information systems and databases from unauthorized users.

5. Policy

5.1 Policy

5.1.1 The Head of IT Department shall approve user id and system access requests via http://apps.mtdgroup.com.my/itadmin/ for non-tolled systems and http://apps.mtdgroup.com.my/badge/ for tolled-systems.

5.1.2   A naming convention will be applied to generate an appropriate user id for the applicant. If access is required to multiple independent computing resources, multiple accounts (based on the same user id) will be created.

5.1.3   With each user id and account, there are a number of privileges that can be acquired to access information systems. Access rights and permissions of resource usage are assigned to the user based on the job description or tasks assigned. Immediate superiors or HOD should indicate this appropriately when requesting for user id and system access request if applicable.

5.1.4   Accounts and user ids are assigned to individuals and are the responsibility of the individual to whom they are assigned. SHARING OF USER ID IS STRICTLY PROHIBITED. User ids are used for security purposes, logging and audit trails. If a user id has been intentionally shared, the owner will be held accountable for any inappropriate or malicious activities tracked back to the user id.

5.1.5   When the user id is no longer required, access to those computing resources must be disabled effective from the last day of service.

5.2   User ID and E-Mail Naming

  5.2.1   User ID Naming

5.2.1.1 Each person will be assigned a user id to be used as a unique identifier for access to all computing resource accounts at MTD.

5.2.1.2 The standard naming convention for creating user id is as follows:
The individual's first name concatenated with the first initial of the middle name (if applicable) followed by the last name will be used.
Examples:
Ahmad Abdullah – ahmad.abdullah
Lee Ming Kee – lee.mingkee
Carrie Tai Wan Chuin – carrie.tai

The examples shown are just as a guide and names used are purely coincidental. In the event that the email address formulated is offensive, permutation of the rule is allowed at the discretion of the individual.

5.2.1.3 All accounts created with this user id should have an expiry date associated.

5.3   Internet Access

5.3.1   The access for the Internet is granted on the position requirement and not to individual. The respective Heads shall submit list of positions that require the internet access in his or her department, division or company to IT department. IT Head is responsible to review the request and submit the request for a one time approval from the Chief Operating Officer (COO) / Chief Executive Officer (CEO).

The approved position list is still subject for a review from time to time. The respective Heads shall approve for an internet access request made by his or her replacement staff if the position has been approved for internet access before. The respective Heads shall submit through IT department for the approval of new positions that have been created.

6. Procedure

Item		Description / Action	Responsibility	Duration / Timeline
6.1		**User ID Issuance**		
	6.1.1	To approve the user id issuance from respective department for onward creation on IT Portal at http://apps.mtdgroup.com.my/itadmin/	Head of ITD	
	6.1.2	To create user id	IT Department System Administrator	
	6.1.2a	To create system access request user id (if applicable)	IT Executive / Sr. IT Executive	
	6.1.3	To configure a PC with the new user id	IT Department IT Officer	Max 2 days
	6.1.4	To brief basic IT facilities to new user *eg: MTD e-mail, MTD website, MFP, network folder (H: & I:), internet restriction and etc*	IT Department IT Executive	
	6.1.5	To acknowledge acceptance of 1.Important Note (Copy Notebook Policy 4.1) 2.User ID 3.IT Asset Issuance 4.Use of IT Policy 5.Letter of Undertaking & Indemnity on IT Portal at http://apps.mtdgroup.com.my/itportal/	Requestor	

Item		**Description / Action**	**Responsibility**	**Duration / Timeline**
6.2		**Internet Access Request**		
	6.2.1	Respective Heads submit list of position for internet access	Respective Heads	Upon Submission
	6.2.2	Review the list of position for internet access	Head of ITD	Max 2 days
	6.2.3	To one time approve or reject the list of position for internet access	COO/CEO	Upon Approval
	6.2.4	To inform Heads for the request status	Head of ITD	1 day
	6.2.5	To approve internet request made by staff	Respective Heads	Upon approval
	6.2.6	To configure internet access	IT Department System Administrator	1 day

Item		Description / Action	Responsibility	Duration / Timeline
6.3		**User ID Termination**		
	6.3.1	To key in the "Effective Date" of the user account termination request upon received clearance form from HCD	IT Department IT Assistant	1 day
	6.3.2	To approve the user id termination request from respective department	Head of ITD	Max 2 days
	6.3.3	To suspend user id	IT Department System Administrator	
	6.3.3a	To disable system access's user id	IT Executive / Sr. IT Executive	
	6.3.4	To check the condition of requestor's PC upon requestor acknowledges return of the PC	IT Department IT Officer	1 day
	6.3.5	To backup user's data to respective department's external hard disk within 4 weeks from the last day of service (applicable to Executive and above)	IT Department IT Officer	1 day
	6.3.6	To acknowledge backup of data	Respective Head	1 day
	6.3.7	To remove the user id after 4 weeks from the last day of service	IT Department System Administrator	1 day

Item		**Description / Action**	**Responsibility**	**Duration / Timeline**
6.4		**ID Activation, ID in-activation, badge card creation, re-badge card creation, activation service (TnG-AC) and to disable service card (TnG-AC) in Toll Collection System (TCS)**		
	6.4.1	• Fill up the request via USER ID FOR *TOLL SYSTEM PORTAL* at http://apps.mtdgroup.com.my/badge/ • The requested services need to be justified by the user Head of Section (HOS)/ Supervisor or Sr. Executive • The approval by HOD/Manager/GM • The request is submitted and emailed to ITD	Requestor	1 WD (Working Day)

	6.4.2	• Processing of task based on service request
		• Service Request include :-
		  ✓ AI-Active New ID
		  ✓ BC-Badge New Card
		  ✓ RI-Reactive ID
		  ✓ ID-Inactive ID*
		  ✓ AS-Activate Service
		  ✓ DS-Disable Service
			TSSM IT Exec	5 WD (Working Day)

	6.4.3	Verification of the completed task	TSSM IT Exec. / Sr. Executive	2 WD (Working Day)
	6.4.4	Approval of the completed task	HOD/ HOS	