

AIMS- ACCEPTABLE USER POLICY

A. GENERAL

AIMS' Acceptable Use Policy ("Policy") provides guidelines for our Customers on the appropriate use of our services, including but not limited to the right to refuse entry, and the right to ask you or your personnel to leave our Data Centre immediately when this Policy has been breached.

Use of our services constitutes acceptance and agreement to this Policy. It is your responsibility to read and understand this Policy.

If you found to have violate our Policy, we reserve the right to suspend or terminate your service without prior notice, and remedy. We prefer to advise you on any inappropriate behavior(s) and any necessary corrective action. However, flagrant violations of this Policy will result in immediate termination of service. Our failure to enforce this Policy, for whatever reason, shall not be construed as a waiver of our rights to do so at any time.

All illegal activities are strictly prohibited in our Data Centre. You shall not commit anything that is illegal which will adversely affect our legal interest or of our customers.

B. DEFINITION

To simplify this Policy, the following definitions shall apply:

The words you, your and yours means all Customers/Persons responsible for complying with this Policy.

The words we, us and our means AIMS, the Service Provider.

C. USE OF OUR DATA CENTRE

1. Entry to our Data Centre
 - 1.1 You must provide us the particulars of your authorized personnel before entering our Data Centre to access your Equipments: -
 - (a) Name;
 - (b) Company;
 - (c) Identification card/driving license/passport;
 - (d) Contact number; and
 - (e) Email address.

You must ensure that the above information is up-to-date at all times, and update us if there is any change.

- 1.2 Prior to entry, you must give a written notice to our Data Centre Operations Engineer (“DC Ops”) at least twenty-four (24) hours before such entry. The notice must state: -
- (a) The date and time of proposed entry;
 - (b) Reason/ purpose for entry;
 - (c) List of equipments to be installed in the customer's space (if applicable); *Equipment Delivery and Removal Declaration Form* is to be completed and submitted to DC Ops;
 - (d) Specific rack number to be accessed; and
 - (e) Names of authorized personnel with relevant information as required in Clause (1) 1.1 (subject to a maximum of 5 personnel per entry).

We reserve the right to refuse your entry to our Data Centre if you failed to adhere strictly to this procedure.

- 1.3 The *One Time Visitor Form* is to be completed if your name is not registered with the DC Ops earlier.
- 1.4 In the event the registered authorized personnel is not present in our Data Centre, the authorized personnel shall e-mail to DC Ops to seek approval for the representative(s)' access.
- 1.5 When visiting our Data Centre, you must register your name at the security department. Upon registration, a visitor pass will be provided. The visitor pass is to be wore through out your visit and visible to us. You will be asked to leave our Data Centre immediately if you fail to produce the visitor pass when requested

D. BEHAVIOUR AT OUR DATA CENTRE

- 1.1 You are prohibited from: -
- (a) Taking photograph;
 - (b) Wearing shoes in our Data Centre;
 - (c) Generating any audible sound and noise from any audio or video sources or act unprofessionally, offensively or inappropriately;

- (d) Eating, drinking or smoking in our Data Centre, washroom, lift lobby or emergency staircase;
- (e) Bringing in any firearms, explosive chemicals or devices, or weapon of any type which will expose all individuals in our Data Centre or the Data Centre itself to any form of danger and risks;
- (f) Opening, accessing, or otherwise interfering any equipments or hardware memory copy of any equipments not belonging to you. You will take full responsibility of any such acts if it causes damage or loss to us and/or our other Customers;
- (g) Blocking, disconnecting, altering the position of any security device such as CCTV and door access cards;
- (h) Breaking the emergency break glass box to exit our Data Centre unless during fire or any emergency.

E. PROCEDURE ON POWER TESTING FOR ANY EQUIPMENTS INSTALLATION AND REPLACEMENT

- 1.1 Prior to any equipment installation and maintenance, you will need to do conduct a power test of such equipment, servers, devices, power adapters and power cord under our supervision at our External Prep Room (located outside of our Data Centre in Ground Floor of Menara Aik Hua) for at least one (1) hour. This is for the purpose of checking the safety of such equipment and the power to such equipment to ensure it will not be disrupted due to any power leakage and/or that power supply to such equipment will not adversely affect the general power supply to our Data Centre.
- 1.2 Upon installation, maintenance or removal of such equipment, *Equipment Delivery and Removal Declaration Form* is to be completed and submitted to DC Ops.

F. POWER AND COOLING

- 1.1 The operation state of any Emergency Power Off (EPO), Valve, Power Distribution Unit (PDU), Computer Room Air Conditioning (CRAC), Fire Alarm Panel, Electrical Panel and related equipments shall not be changed and touched at all times as these actions may disrupt the entire operation of our Data Centre.

- 1.2 The following actions are not allowed: -
- (a) Installing Rectifier and independent standalone small scale Uninterruptible Power Supply (UPS), unless pre- approved by us;
 - (b) Any modification on the rack's power socket strips configuration;
 - (c) Installing extreme high power density (kW) equipment unless pre-approved by us;
 - (d) Installing heavy equipments of more than 500kg, unless pre-approved by us;
 - (e) Carry out power testing in the rack by using multi-meter, mega-meter and other instrument; and
 - (f) Injecting fault current, short circuit equipment, tripping tester.
- 1.4 Prior to installation, Equipment Power Health Test must be conducted. All equipments that are to be installed including PDU strips, power cord and others must comply with our technical guidelines and specifications, and also the standards and requirements from the local authorities' such as SIRIM, Suruhanjaya Tenaga and so forth for safety reason.

G. OTHER RESTRICTIONS

- 1.1 You are prohibited from: -
- (a) Pulling data cabling from one rack to another. All circuit cross-connects from rack to rack shall be carried out by us or our authorized contractor;
 - (b) Connecting/ disconnecting/ altering any cross connection on the Meet-Me Patch Panel;
 - (c) Removing any raised floor tiles unless authorized by us;
 - (d) Drilling or penetration to the racks, tiles and walls; or
 - (e) Damage any fire detector, gas suppression pipe or HSSD pipe during your equipment installation.

H. FIRE SAFETY PROCEDURES

- 1.1 Our Data Centre is equipped with Clean Agent Gas Suppression System. You are strictly prohibited from carrying out works such as soldering, welding and

drilling in our Data Centre as the smoke and dust emitted from such works will cause the smoke detector to be activated.

- 1.2 In the event your equipment catches fire, you must inform our personnel immediately and evacuate yourself from our Data Centre.
- 1.3 In the event of fire, you must remain calm and evacuate immediately through the nearest exit. Follow the "KELUAR" sign to exit the Data Centre. You are prohibited from re-entering the Data Centre without clearance from us. When the alarm bell is activated, the access door will open by itself. If the access door fails to open automatically, please use the "break glass to open door" device for manual override. Do not use the lift in the event of fire.

I. INTERNET ACCESS

We do not provide internet access but we may subscribe such services on your behalf. Any internet connection provided by 3rd Party, shall be governed by their policy.

J. SEVERANCE

If any provision in this Policy or part thereof shall be void for whatever reason, the offending words shall be deemed deleted and the remaining provisions shall continue in full force and effect.

K. REVISION OF THIS POLICY

We reserve the right to add, delete, modify any provision of this Policy at any time without notice. Please log onto <http://www.aims.com.my/pages/customer-service/downloads.php> periodically for the most recent revision of this Policy or contact our personnel for the latest copy.