DC Rules of Conduct and Safety

ETISALAT DATA CENTER- V2.9

DOCUMENT NUMBER: DCS20160831

DATA CENTER INFRASTRUCTURE

Public Document

Aug-2016

Document Information and Revision History

File Name	DC Rules of Conduct and Safety
Original Author(s)	Salma Al Nuaimi (SM / Data Centre Colo-Support)

Version Control

Version	Date	Author(s)	Revision Notes
1.0	25/05/2012	SM-DCS/Salma	Initial Draft
1.2	30/06/2012	DCS/Danish	Draft based ISO format
2.5	03/02/2013	DCS/Mohammed	Installation policy update
2.5	14/04/2015	DCS/Danish	Violation & Rules of regulations update
2.6	04/06/2015	D-DCI/Salah	update
2.7	06/12/2015	DCS/Salma	Update Installation Procedure
2.8	31/05/2016	DCS/Salma	Added staging/store use procedure
2.9	31/08/2016	DCQC	Updated under 5.5

Document Approval

Name	Designation
Salah Al Sadqi	Director / Data Centre Infrastructure
Salma Al Nuaimi	SM / Data Centre Colo-Support

Distribution List

#	Name / Team
1	eHosting Customers
2	Etisalat Internal Team

Table of Contents

1.0 Definitions

Contract Is the direct contract between a Customer and Etisalat for the use of Data Center Hosting Services

Customer Shall be deemed to include the Customer and their valid employees, agents and contractors and any other person entering the Data Center on behalf of the customer.

Customer equipment shall mean the Equipment provided by the Customer for hosting at the Data Center

DC "Data Center", Shall refer to Etisalat hosting facility which contains IT and Telecomm equipment where the contracted area is located.

Etisalat Data Center Any Equipment which is supplied by or on behalf of

Equipment Etisalat Data Center to the customer

End User Any person or entity using the Data Center facilities but without a direct contract with Etisalat for the use of such facilities, including but not limited to the customers.

Contracted Area Is the rack (or part thereof), cage area provided to the Customer for its use as stated in the relevant Order Form.

24/7 Indicates that Data Center is operated 24 hours a day, 7 days a week

2.0 Introduction

Etisalat Data Center rules of conduct and safety are in compliance with the e-Hosting and Co-location best practices to ensure service availability and reliability for Data Center customers.

The rules are strictly applied to all site entrance in order to ensure and maintain safety and security of individuals and equipment in Etisalat Data Center (ISO27001, ISO22301 BCMS etc. standard).

Etisalat Data Centre Rules, may be updated, modified or supplemented from time to time, the customers will be notified for such change, state the general rules governing the Customer’s activities within the Data centre. These rules shall form part of the contract.

In case of any conflict between the terms of this set of Data Centre Rules and any other term of such Contract, the terms of the contract and its terms and conditions shall prevail.

3.0 Safety Instructions

Safety measures have been taken in Etisalat Data Center in order to minimize the exposure or risk on Data Center visitors. However, the Data Center is an engineering facility; consequently, entering the facility visitors may be exposed to safety hazards including but not limited to the following:

- **Excess noise level:** potentially causing damage to hearing. Customers are advised to minimize exposure to excess noise levels where possible.
- **Open electrical wiring:** open power supply boards or other potential electrical shock hazards. Customers must adhered with such hazards, which may potentially cause serious discomfort, injury or even death.
- **Open floor tiles:** In order to open floor tiles for maintenance or other purposes, need to obtain an approval from onsite Support team; Customers should take care not to fall in to or over the floor openings.
- For safety, Customers must closely abide by the Data Center team instructions with respect to safety on site.

3.1 Multi Physical Security Levels

- Etisalat Data Centers are secured facilities. Access to the data center and other areas of the facility are restricted to those persons with authorization. Customers are restricted to authorized areas only, including the lobby, customer lounge, conference rooms, common areas, and customer hosted space on the data center floor.

- Security controls include 24 x 7 security officer presence, sign-in procedures, managed key and access card plans, mantrap, managed access permissions and access request methods.
- Closed-circuit television (CCTV) cameras are used to monitor all areas of the facility including lobbies, common areas, customer lounge, data center floor space, admin areas, and engineering plant areas for your safety. All CCTV cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.
- Etisalat Data Center Doors provided with Surveillance Access Control Security system.
- Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited, Defaulter may face Legal liability concerns as per UAE law.
- Exterior Data Center doors may not be propped open. These access doors are Monitored and alarmed.
- **Data Center Team reserves the right to access any part of the Data Center at any time for safety /emergency/Hazardous conditions and security reasons, which will be intimated to customer notice.**
- **Data Center staff is authorized to enter customer cages/enclosure for routine site health check/audit purpose along with proper customer notification/approval in order to provide quality services.**

3.2 Upon entering the Data Center

- Note carefully the Data Center plan with respect to the emergency exits.
- In case of FIRE/EMERGENCY, leave the building IMMEDIATELY. Please read the instructions at the entry/exit of the room to identify where the nearest escape route is. Assemble on the assembly point as issued by designated Data Center staff. Do not leave the facility without notifying the designated onsite staff.

- Customer must adhered to rules of conduct and safety signage at the entrance of Data center equipment room.
- Data Center ceilings are fitted with FM200/inergen/argon gas for fire suppression. After the detection of fire, the alarm will start immediately; customers have to leave the room as soon as possible before the gas is enabled.
- Manual Fire distinguisher being distributed at Data center floor in designated area for manual intervention
- In case of emergency, contact the onsite Data Center staff immediately.
- Smoking is not permitted at any time in the Data Center building.
- All kind of food and beverages are not permitted in the Data Center equipment room.
- Customer shall take full responsibility for any actions, misconduct, etc. of their employees/vendors while on Data Center premises.
- All customers of the data center are responsible for maintaining the cleanliness of the inside and surrounding area of their cabinet and/or cage. All wire, cable, insulation, paper, plastic or other scraps Materials must be removed and carried outside the data center for proper disposal.

4.0 Privacy Notice / Camera Surveillance

- The Data Center is equipped with permanent visible security cameras for video surveillance and registration.

- The security camera images are recorded for the purpose of surveillance of unauthorized access, security, safety and registration of misconduct.
- Camera recordings are stored for a maximum duration of 1 month, except for recorded incidents, which may be stored for as long as required to resolve or deal with any incident. Camera recordings can be used as evidence by Etisalat Data Center in any legal proceedings.
- Cameras are used to monitor all areas of the facility including lobbies, common areas and Data Center floor space. Violations noted by cameras will be addressed promptly.
- Customers who want to make use of their own camera systems to monitor their equipment **may do so upon receiving the Data Center approval. However, they are only allowed to do so within their racks and the camera should not be pointed outside the rack or at anywhere else within the Data Center. Etisalat Data Center team shall be entitled to require the repositioning of Customer cameras where these are not correctly placed.**
- Photography/filming inside the Data Center is strictly prohibited.
- No CCTV footages will be allowed to be watched/reviewed by Customers as its security breach. In case of any incident/circumstance based on Data center approval report will be shared with end users.

5.0 Access, Deliveries and Change Management

5.1 Data Center Access List Management

- All Customer’s staff/vendor/contractor shall conduct themselves in a courteous professional manner while visiting the Data Center facility. Customers shall refrain from using any profanity or offensive language.
- Customers must follow the Data Center access procedures at all times when visiting the Data Center. Etisalat Data Centers have a restricted access policy. Customers have to adhere to Etisalat Data center access policy and procedures.
- Customers may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
- Customer shall take full responsibility for any actions, misconduct of his staff/vendor/contractor while on Etisalat premises
- Data Center requires a written submission of customer authorized list upon signing eHosting agreement with Etisalat (for who has permitted to access his hosted equipment within Etisalat data centers).

- **Customer Access Authorization Sheet has to be signed and stamped with customer seal signature in order to process the authorization request.**
- Customers are responsible for maintaining updated authorized list. Any modification (additions/deletions) of the list should be addressed to the Data Center in writing.
- Only Individuals identified on the list will be granted access to the Customer's Sub Rack, Cabinet or Cage. The Customer remains responsible for their activities.
- Data Center shall not be held responsibility for the activities carried out by individuals whose authorization are revoked and not updated to Data Center by customer. Customer should update/ reconfirm his authorization list on routine basis.
- In all time, access request for authorized/unauthorized representatives of the Customer may be allowed to access the Data Center facility subject that their names, date and time and purpose/scope of the visit is shared with Etisalat Data Center Support team via the support portal ticketing system, prior to their visit.
- Customer must obtain approval from onsite Data center support team for created access request prior to approaching the DC premises for planned/unplanned access.

5.2 Data Center Entry/Escorting Procedure

- Customer and their authorized representatives may access the Data Center facility 24/7 upon logging ticket through support portal.
- Customer should provide data center staff with information of his activities that he is going to carry inside the data center.
- Work or visits must be announced in advance (at least 24 hours) and registered with the Data Center support team through support portal (https://si.etisalat.ae).
- If customer is facing any login issues on the support portal, access request can be sent to Data Center Support mail (support@dc.etisalat.ae). Then, Data center Support team will raise access ticket and will reply to customer mail with SD reference number. **Customer may contact Data Center Support team for follow-up on toll free number 8004181 (within UAE) or +971 4 8004181 (overseas customer).**
- During provisioning/ installation stage for new customer, access request can be raised for one week or more subject to approval.
- During provisioning/ installation stage, access request can accommodate maximum 10 visitors/ personnel per activity/visit. If more visitors required then approval to be obtained from data center team with proper justification.
- For operational Customer, access request to be raised for each day (each ticket valid for one day). However, access can be extended for maximum one week upon Support team approval.

- **For operational customer, each access request can accommodate maximum 5 visitors/personnel per activity/visit. If more visitors required then approval to be obtained from data center team with proper justification.**
- In case of emergency, authorized persons will be granted access and Data Center team will assist them to open a ticket on their behalf.
- Cabinets and cage keys shall be held with Data Center support team. Customers must return the key(s) to the Data Center Support team at the end of each visit to the Data Center.

- All persons entering the Data Center must:
  - Valid Service Desk ID i.e. #SD******
  - Possess a valid government issued photo ID (e.g. Emirates ID/Driving License).
  - Have authorization to access the facility.
  - Log in and out when entering the facility indicating the purpose of the visit.
  - Submit all access cards, keys, and Data Center owned tools prior to exiting the facility.

5.3 Deliveries

- The Data Center delivery timing is from Sunday to Thursday between the hours of 8 AM and 2 PM UAE local time .**However, Subjected to approval, delivery of shipment may extended to 24x7.**
- In case of an emergency an approval must be obtain from Data Center Team.
- Customers shall provide at least 24 hours' notice prior to any delivery and/or loading.
- Customers must attend to facilitate such delivery/loading/ offloading.
- Data Center team may agree to receive goods on behalf of Customers, Data Center team shall not be liable for any damage to such goods and sign delivery notes on behalf of Customer provided that it will not be responsible or liable for any incorrect deliveries, damaged content or packaging.
- All packages shipped to the Data Center must include customer name, contact details and location details on the shipping label or it will be refused.
- Delivery should take place within the hours of 8 AM and 2 PM local time and can only be accepted by designated Data Center staff (not the Security guards). **Else, Prior approval to be obtained**
- Other than the acceptance of deliveries under this clause the Customer shall be solely responsible for the delivery;
- **Customer is responsible to provide Labor resources for offloading and uplifting big shipments to designated loading/staging area and to arrange unpacking and installation of their equipment.**
- Trolleys will be provided by the Data Center staff for transporting the Customer Equipment within the Data Center, provided that such trolleys are returned to the designated trolley storage areas immediately after the Customer has finished transporting the Customer Equipment to his contracted area.
- Customers must make sure that the delivered equipment is installed at the same date. Otherwise, Customers will have to take uninstalled items back.
- Delivered equipment/item should be un-packed at designated area named as staging room/area.

5.4 Use of DC Facility staging /Store room

- Staging room is shared designated area to be utilized for unpacking/ unboxing delivered equipment to the facility, on a first-come, first-served basis. Customer should move the delivered items/equipment from loading pay to this designated area to do all unpacking.
- Customers are not allowed to store/keep any equipment's in the DC Staging room without prior permission from Data center team. Delivered items should be installed at same day.

- However, subjected to approval and based on space occupancy, staging room can be used as temporary storage during initial provisioning phase for one-week period. Approval to be obtained for extended period.
- Staging areas also, offered customer a convenience space for configuration/testing of servers prior installing/mounting in the subscribed hosted data center colocation white space.
- Customers are allowed to use test cabinets available in the DC Staging room facility for testing and configuration of equipment's before going live.
- The staging room should be maintained clean and tidy. It should be free from empty boxes, waste, packaging and other unwanted materials.
- The doors of the DC staging room should always keep closed. Only customers and their authorized representatives may access the staging/storage room facility upon informing DC security.
- Customer should follow good cleanliness practices while using the staging room facility, should dispose all empty boxes, packaging, waste and other unwanted materials from staging room to designated area before leaving the DC Site.
- Customers may use DC Smart tools kept in a staging room facility upon informing DC security and should return it after the completion of work.
- Customers should make an entry in DC Smart Tools log book while taking the tools and returning the tools. DCS team and DC security should make sure that the customer returned the tools and made the entry in the logbook.
- Customers should return the tools used by them in the same condition as it was before. DCS team reserves the right to claim any damages caused to the tools or other staging facilities by the customer/vendor.
- Customers should take out all equipment's/items that belong to them out of the DC staging room upon expiry of the granted approval.
- DCS team reserves the right to remove/clear the customer equipment's/items out of DC staging room if the customer does not take out their equipment's/items that belongs to them beyond the allowed period after several notifications.
- Customer should provide clear labeling/marking for his temporary stored packing materials kept at staging room or storeroom.
- Further, Customers are allowed to use temporary DC Store room for keeping their delivered materials on a temporary basis for maximum of one-week period, which is subjected to prior approval from data center team and upon space availability, during provisioning /projects.
- The doors of the DC Store room facility should always keep closed and locked. Customers are not allowed to enter/use DC Store room without DCS team presence.
- Customer should provide clear labeling for his temporary stored materials kept at storeroom.
- Customers are not permitted to approach, inspect or examine any equipment items/property kept in the storeroom that does not belong to them.
- Unauthorized persons/visitors are not allowed to enter DC Store room facility.
- DCS team reserves the right to remove/clear the customer equipment's/items out of DC store-room if the customer does not take out their equipment's/items that belongs to them beyond the allowed period after several notifications.

5.5 Change

- All changes (i.e. adding, removing, re-allocating of equipment) within the Data Center are subject to approval of Data Center team.
- 24 hours notification is required to remove/replace/add any equipment, **in case of emergency** need to obtain an approval from Data Center Team.
- Delivery of approved Changes, should take place within the hours of 8 AM and 2 PM local time. However, installation & configurations of those changes may continue to be during non-business hours subject to data center team approval.
- In case of emergency, customer may allowed, to deliver, install & configure his devices during non-business hours subjected to prior notification and approval from both DCCS/DCCO on valid register SD tickets.
- Customers should open a ticket on the support portal for removing/replacing and adding any equipment within their contracted space or rack.
  - Customer has to fill Data Center Installation Checklist Form upon arrival (not after completing activity) to the site.
- Upon cessation of the service, Customers must leave the space or rack in good condition as it was at the commencement date.
- Data Center shall be held no responsibility whatsoever with regards to any hardware or any items left by the Customer after two weeks from the service cessation date.
- Installation or removal will not be permitted with in the Data Center without prior approval from the Data Center team.
- At the time of cessation customer must remove all his/her belongings from Etisalat Data center prior to leaving the premises. Etisalat will be hold no responsibility whatsoever with regard to any hardware, belonging or any item left by the Customer in the Data Center from the service cessation date due to termination or expiry of the Agreement. If the Customer, at its own cost, fails to remove their Equipment and Customer's data on any leased Equipment within thirty (30) days of the contract termination, then, Etisalat will have the full authority to dispose and/or use such Equipment as it deems fit.

6.0 Rack, Cage and Customer equipment

- Customers shall ensure that the Customer Equipment conforms to the current Data Center standards and is in good operational condition. Installation of Customer Equipment shall at least comply with:
  - Etisalat Data Center Standard with in this document.
  - ITIL standard
  - TIA 942 - best practices, commonly applied within Data Centers.
- Customers shall ensure that the Customer Equipment and surrounding area do not pose safety hazards to any persons or equipment. This includes (but is not limited to):
  - Exposed AC/DC electrical hazards
  - Optical or radiation hazard

  - Trip and slip hazards
  - Hazardous materials
  - Improperly secured or overloaded racks, ladders or inadequate ingress and egress space.

- All Customer Equipment and cabling must be securely installed within the contracted Area.
- All racks doors should be closed if not (actively) under installation. Customers must close and lock all their racks before leaving the Data Center.
- No free-hanging cabling (including cable loops) is permitted, and all such cabling connecting to the Customer Equipment must be securely tie-wrapped within a cable management system attached to the standard Rack. Any cabling outside the contracted Area must be approved by and carried out by the Data Center staff or their designated contractors.
- Customers are prohibited from plugging their own power strips into the contracted rack power distribution units; it is the violation of electrical and safety codes and the Data Center reserve the right to remove it.
- Customer Equipment and its associated items of any kind must be in the contracted Area and must not extend into or interfere with the rack space or cage of any other Data Center Customer or Etisalat Data Center.
- Un-racked equipment is strictly prohibited in or outside the contracted area.
- Customers with Cage subscription must label all Customer Equipment and cabling and other associated equipment to enable the Data Center staff to adequately identify the Customer Equipment.
- The initial installation and final removal of the Customer Equipment must be coordinated with and agreed to in advance by the Data Center staff.
- Customers should contact Data Center staff for assistance in case locks or doors are not functioning properly.
- Customers are prohibited from lifting or removing floor tiles inside their cage without prior approval from the Data Center staff.
- The creation of office space within the contracted area on the Data Center floor is prohibited.
- Any kind of installation should be advance or appointment basis with onsite Data center team.
- Installation check list form must be filled/submitted on exit from white space
- Fillers/Blanking panels must be installed in the free U's of the cabinet in order to maintain the airflow. In case of non-standard cabinet/cage subject to approval from Data center team.
- In case of customer's owned cabinet installation perforated doors must be installed in order to maintain airflow with in the Data Center white space.

7.0 The contracted area and the Data Center facility

- Customers must cooperate and obey all reasonable requests of Data Center personnel while within the Data Center, including immediately addressing any violations of rules when brought to Customer's attention.
- Customers must not conduct any act that may adversely affect the provision of Etisalat Data Center services or damage the property of any other Data Center customer.
- Customers must take all necessary safety measures to protect the walls, floors, ceiling and Data

Center Equipment or furniture or any other property held in the Data Center and any equipment belonging to other customers or Data Center from any physical damage whilst installing or moving the Customer Equipment.

- **Data Center reserves the right to claim any damages to the Data Center or any Etisalat Equipment or furniture or other third party property caused by Customer/vendor.**

- The Customer acknowledges that the Data Center is protected by a smoke detection system and an inert gas fire suppression system (FM200/Argon/Inergen gas) and the Customer agrees that it shall be liable for any costs and expenses that result from any activation of such systems due to Customer activity that is in breach of these Data Center Rules and/or the terms of any Contract including but not limited to, the cost of replacing such systems.
- Customer shall follow good cleanliness practices whilst in the Data Center.
- Any waste, packaging or empty boxes or any other items stored outside of the Contracted Area Data center team reserve the right to remove in order to maintain healthy environment of the Etisalat Data Center.
- No food, beverages or liquids of any kind shall be allowed in or around the Contracted Area or elsewhere in the Data Center except that eating and drinking is permitted in the designated areas. Smoking is not permitted anywhere in the Data Center.
- Ladders/Chairs/table not be permitted in any designated areas without the prior consent of the Data Center team.
- No corrosive, combustible or hazardous material must be stored in the Licensed Area or elsewhere in the Data Center.
- The Customer must not interfere with any equipment, items or property at the DC other than Data Center Equipment and/or the Customer Equipment contained in its Contracted Area. In particular, the Customer shall not interfere with any overhead lighting, cabling pipes, and data cabling baskets, floor tiles or power provisioning or access the floor voids without the prior permission of the Data Center staff.

8.0 Installation Policy

8.1 Racks specification

- **Open frame racks structure are not allowed for hosting IT equipment within Etisalat hosting Data center as its not providing a physical equipment security & they offer very little control over airflow.**

- **Customer should supply Rack enclosure (Rack Cabinet) type with fully ventilated front and rear doors with door locks & Solid side panels and rolling wheels. Using Glass doors or Doors with low ventilation is causing overheating and affect are circulations. Thus, Mesh or perforated doors should be used on the front and rear of all customer cabinets.**

- **The front and rear doors are typically ventilated to encourage ample airflow from front to back, through any installed equipment in order to manage cooling airflow & Solid side panels prevent hot air from recirculating around the sides of the enclosure.**

- **Closed Rack cabinet are ideal for applications that require heavier equipment, hotter equipment and higher wattages per rack & also provide physical equipment security at the rack**

- **The industry best practice is to arrange Racks in a hot-aisle/cold-aisle configuration to enhance equipment performance and life. This arrangement prevents hot air that has been expelled from one equipment rack to be drawn into equipment directly across the aisle. This practice optimizes cooling efficiency, extends equipment life and reduces potential damage from overheating.**

- **Customer supplied rack must have adequate height/depth/width/load bearing as per etisalat hosting guidelines**

- **The height of the rack will determine how many rack spaces (U's) are available for hosted devices/ equipment & will be considered for leaving extra space for horizontal cable managers, future expansion or other purposes. Common heights for floor-standing racks and rack enclosures are 42U, 45U, 47U and 48U custom.**

- **The standard width for rack enclosures is 24 inches or 600 mm, which corresponds to the standard for removable floor tiles in a raised-floor data center. Rack with extra width have more side channels to accommodate high-density cabling and cable managers without obstructing airflow.**
- **The rack's depth is important to make sure it will be deep enough for the equipment, including any cabling that extends past the equipment cabinet.**

- **The load rating (or weight capacity) of the rack is how much weight it can safely support. Racks should be chosen to meet the capability of required loads.**
- **The allowed Customer own Supplied Rack enclosures(Cabinet) as per Data Center standard rack size:**
  - 600mm x 1000mm or 800mm x 1000mm
  - 600mm x 1200mm or 800mm x 1200mm
- **All racks should be installed as per Data Center staff instructions to maintain the cold and hot aisle design.**
- **Customer should mount his devices in the rack as per hot/cold aisles arrangement. Device front side should face cold aisle and rear side should face hot aisle.**
- **Customer is not allowed to cut the tile under his rack; customer should request the Data Center for tile cut.**
- Its mandatory for customers/vendor to use **seal/cover** the tile cut under his rack **using brush strips/ grommets to block air leaks around cable channels and other gaps.**
- It's mandatory for customers/vendor to fix/cover empty space within the racks on using blanking panels/filler **to prevent hot air from recirculating through open spaces.** All unused RU spaces must be filled.
- **Customer must extend earthling for all his cabinets/Racks (Mandatory), in case of any assistance please refer to onsite data center team.**
- **To eliminate hot spots within the cabinet, fans can be placed on top of cabinet to direct the hot exhaust out of the cabinet and into a hot area.**

- **All Rack components, including the roof, doors, rails, side panels and frame should be grounded for safety.**

8.2 Servers and other equipment

- Customer should follow Data Center onsite staff instructions when installing new equipment inside the Data Center premises.
- Installed equipment in the Data Center must be clearly labeled with the code name provided by the Data Center staff.
- Customers are allowed to install rack mounted equipment only. In case of non-standard equipment, customer should arrange rack shelves in line with respective account manager.
- Customer should provide the correct power cable type as per the Data Center standard rack power distribution unit or ASHRE standard.
- **All servers should be placed 4 to 6 inches from the front and rear cabinet doors to provide sufficient space for accessories, such as handles and cables, as well as airflow.**

- Customer is not allowed to leave any server or device on the floor outside the rack.

8.3 Cabling

- **Cable management can have a negative impact on cooling if not properly structured and maintained. Poor cable management can lead to poor airflow, excessive heat absorption, and increased cold air bypass.**

- **Customer must adapt Good Cable Management which can be Attained When Cables are neatly contained and bundled when possible, Correct cable length is used, and cable slacks or unneeded loops are avoided, Air blocking devices are used around all cable egress points**

- **Install equipment to promote shortest cable routes. Avoid large slack bundles which adsorb heat and block airflow. • Avoid cable arms that block rear exhaust airflow.**

- Unless otherwise agreed, only Data Center or its suppliers or subcontractors are allowed to perform cabling activities within the rooms, cages and the general collocation facilities. Customer or its suppliers are allowed to perform cabling after Data Center approval and under Data Center staff supervision.
- Customers are allowed in the cage area to perform in rack cabling or cabling between its adjacent racks.
- Direct Interconnection between the Customer and any other Data Center customer is **not allowed** without prior approval. Customer should contact his account manager to request for interconnection between his equipment and any other Data Center customer. Data Center allowed only interconnecting two customers as per the work order.
- All connection to and from customer equipment must be **clearly labeled.**

- All cabling performed without the written approval from Data Center will be deemed unauthorized and can be removed by Data Center without prior notice. All costs involved in the removal of such cabling shall be billed to the Customer. Customer cannot claim any loss or damages due to the removal of such cabling and Data Center shall not be liable to the Customer for any such removal.
- Customer should use the right cable length prior to using it and they have to consult the Data Center team for possible solution.
- Data cables must be separated from the power cable in customer's cabinet. Data Center staff can be consulted for solution or advice.
- Customer must supply and use proper cable lengths and avoid using long curved cables .

9.0 Technical Limitation

Weight: Floor load should not exceed approved distributed load.

Power: Hosting packages cabinet that are connected to PDU via a 230V/16A circuit breaker (default configuration), with two feeds (A and B). Other power configurations should be available upon request and where agreed to by Data Center.
Hosting packages cabinet socket type is 13A UK standard socket or IEC 309 16A, 32A and 64A Industrial sockets and other type of sockets prior to Data Center approval.

9.1 Power usage limitation

- Hosting packages cabinet are fed by a 230v/16A circuit breaker in 2 x 230v16A circuit breakers in a redundant feed (A+B) feed configuration.
- To prevent tripping of the circuit breaker in case of a rest (after outage) the power usage per circuit breaker should not exceed 80% of its capacity.
- When a rack is supplied with a redundant feed, Customer must distribute the power consumption evenly over both feeds. In this case, the maximum current (max) of combined power feeds should not exceed 14A for the standard Data Center rack.
- In case of a tripped circuit breaker, the Customer will be deemed to have overloaded the power feed. Accordingly, the Customer must remedy the overload. The circuit breaker will then be reset. The Circuit breaker is the interface point between the guaranteed Data Center power distribution and Customer Equipment.
- Regardless of the available power plugs in the cabinet, no further equipment shall be installed in the Data Center if power utilization reached 80% of the UPS capacity.

Heat dissipation: differ from one site to another, as per the Data Center cooling design (watts per/sqm). This means a cabinet will be deemed full if the agreed limit is reached, regardless of the available space in the cabinet and no further equipment shall be installed in such cabinet which would increase the heat dissipation above such level.
Temperature: Under normal climatic conditions the general temperature in rooms with generic room cooling is 18 to 27 C ± 5 ° and differs from one site to another as per the cooling design in each site as per ASHRE standard.

10.0 Violation of Rules and Misconduct

- If Data Center staff notifies Customer in writing of a violation of the Data Center Rules, or any other unsafe or unacceptable situation or practice, the Customer must resolve the problem within 24 hours or provide a written undertaking and plan for resolution to the Data Center satisfaction and a proposed correction date. If the problem is not resolved in 24 hours or within a longer time period as agreed by the Data Center, the Customer will be deemed to be in material breach of the Contract and Data Center will have the option of either:
    - correcting the problem at Customer's expense
    - or taking such remedial action as provided for in the Contract, including, without limitation, suspending
    - or cancellation of the Service
- Major violations as determined by the Data Center, are subject to immediate correction by the Data Center without prior notice to Customer.
- Corrections made by the Data Center are at the Customer's expense and will be billed to the Customer on a time and materials basis where appropriate.
- The Customer may be denied access to the Data Center where it fails to follow the Data Center rules or directions from the Data Center staff.
- Please do not drag equipment over the raised floor. Please use a transportation device with rubber wheels. No steel wheels pallet jacks are allowed on the raised floor unless adequate protection (cardboards) is in place to protect the floor.
- The use of devices such as vacuum cleaners, drills or similar are not allowed in the raised floor area.
- Etisalat reserves the right to inspect all objects to be brought into or taken out of the Data Center and to exclude from the Data Center all objects which violate any of these rules and regulations.
- A Customer is not permitted to approach, handle, use, inspect or examine any equipment, cabinets, cage space, other than their cabinets.

11.0 Annex:

11.1 General Policy Note on Visitor Access

- The Customer must follow the Visitor Access Notification procedure at all times when visiting the Data Centre.
- Data Center is operated 24/7, hence access can be granted any time.
- Customer should open ticket on https://si.etisalat.ae for any kind of visits and get the approval before visiting the Data Center.
- All visitors are registered, coming in or going out of the facility.
- The Data Center is monitored by security cameras for surveillance and security purposes, all images are processed and recorded.
- Whilst leaving the Data Center, the access passes and/or keys are to be returned to the Data Center staff.
- The Visitor agrees to only enter and exit the Data Center through the designated access areas as notified.

11.2 Authorization of Access – Setting up Access – Authorization list

- Only main authorized contact person are able to grant or withdraw unescorted access rights to the Contracted area.
- Main authorized contacts are required to be full-time employees of the Customer, not of a third party and shall be listed in the authorization form.
- At least one Main authorized contacts should be available/reached 24 x 7 hrs. to validate access requests.
- The Authorization list is to be maintained by a duly authorized Customer representative as listed in the Company main authorized list contact. It is the Customer's responsibility to keep the authorization list up to date.
- Every change to the authorized list is acknowledged by the Data Center returning the updated list to the Customer after each change. Data Center aims to make any change within 1 working day of having received notice of such change.

11.3 Revoking Access

- EMERGENCY: In case of revoking Access or Authorization privileges, it would processed based on customer request.
- Revocation of access can only be performed by Customer authorization form.
- Revocation of an authorized contact can only be performed by a duly authorized Customer Representative as listed in the Company authorization form.
- Revocation of access can be done on priority basis based on customer request
- The Company may refuse entry to, or require the immediate departure of, any individual who:
    - is disorderly,

- fails to comply with this Data Center Use Policy,
- Fails to comply with any of company's other policies, procedures and requirements after being advised of them.

11.4 CONDUCT GUIDELINES

- Customers may not misuse or abuse any company property or equipment.
- Customers may not verbally or physically harass, threaten, intimidate, or abuse any individual within the DC including without limitation, employees, and agents, 3rd party vendors of the Company or other visitors.
- Abusive and threatening or offensive behavior by any visitor will not be tolerated and legal liabilities will be applicable as per UAE law.

11.5 MODIFICATIONS OF POLICY

Etisalat reserves the right to modify this Policy at any time without notice. We will attempt to notify our customer of any such modifications either via e-mail or by posting a revised version of the rules of conduct & safety on our Web site. The customer/clients/end-user have the obligation to check our website page from time to time, to take notice of any changes; as such updates are legally binding the clients. Some of the provisions contained in this Policy may also be superseded by provisions or notices published elsewhere on our site or written documents issued to you.