DC Rules of Conduct and Safety

e& enterprise

DC Rules of Conduct and Safety

e& enterprise DATA CENTER V.3.4

DOCUMENT NUMBER: DCI20180322

DATA CENTER INFRASTRUCTURE

Public Document

May-2022

e& enterprise

Document Information and Revision History

File Name	DC Rules of Conduct and Safety
Original Author(s)	Salma M Al Neaimi

Version Control

Version	Date	Author(s)	Revision Notes
1.0	25/05/2012	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/Alqadi	Updated under 5.5
2.10	30/07/2017	DCS/Salma	Updated-8.1(Earthing of customer cabinet) Updated 7.0 & 10.0 (Violations of rules)
3.0	10/12/2018	DCQC, SD/DCI, DCMOC	-Emergency Response Plan added. -HSE instructions, -DC certificates update -Annex# 12 updated, -Section 8.3 updated
3.1	03/03/2020	DCQC & DCS Teams	Section 5.0 ,8.0,9.0 updated
3.2	27/05.2021	DCQC Team	Section 1.0, 3.1, 4.0, 5.0, 5.2, 5.4, 6.0,9.1, 10, 11.4 and 12.6 Updated
3.3	14/11/2021	DCQC Team	Section 12.7.7 Access protocol during pandemic Added
3.4	25/05/2022	DCQC Team	-Section 5.3 Updated as per the New Weekdays -Format Changed -Covid access protocol updated

Document Approval

Name	Designation
Salah Al Sadqi	Sr. Director / Data Center Infrastructure

Distribution List

S. No.	Name / Team
1	DC Hosting Customers
2	e& enterprise Internal Teams

e& enterprise

Table of Contents

1.0 Definitions

The following terms shall have the following meanings assigned to each of them in this document:

- **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.
- **Data Center:** shall mean the colocation facilities and location provided by e& enterprise including physical security, power supply, controlled environment & colocation network infrastructure.
- **Contract:** Is the direct contract between a customer and e& enterprise for the use of Data Center Hosting Services
- **Customer equipment:** shall mean the Equipment provided by the Customer for hosting at the Data Center
- **e& enterprise Data Center Equipment:** any Equipment which is supplied by or on behalf of e& enterprise Data Center to the customer
- **End User:** any person or entity using the Data Center facilities but without a direct contract with e& enterprise 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
- **Incident:** A work-related event(s) that doesn't result in serious injury or illness but may result in property damage.
- **Accident:** a work-related event(s) in which an injury or ill health (regardless of severity) or fatality occurred, and also result in property Damage.
- **Risk:** a source, situation, or act with a potential for harm in terms of human injury or ill health or a combination of these.
- **Hazard:** a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of the injury or ill health that can be caused by the event or exposure(s).
- **Emergency:** Any event or emergency that interrupts or halts the operations of the Data Center
- **Incident Response Procedures:** Written document(s) of the series of steps taken when responding to incidents; Combination of incident response policy, plan, and procedures.
- **Information Security:** Preservation of confidentiality, integrity, and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

2.0 Introduction

e& enterprise Data Center's 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 entrances in order to ensure and maintain the safety and security of individuals and equipment in e& enterprise Data Center (ISO27001, ISO22301 BCMS, etc. standard).

e& enterprise Data Center Rules may be updated, modified, or supplemented from time to time, the customers will be notified of such change, and state the general rules governing the Customer's activities within the Data Center. These rules shall form part of the contract. In case of any conflict between the terms of this set of Data Center Rules and any other term of such Contract, the terms of the contract and its terms and conditions shall prevail in the order in which they appear in the Agreement.

3.0 Safety Instructions

Safety measures have been taken in e& enterprise Data Center in order to minimize the exposure or risk to 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 adhere to 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 approval from the onsite Support team; Customers should take care not to fall into 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

- e& enterprise 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 captured by camera/ any other media will be addressed promptly.
- 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.
- e& enterprise Data Center doors provided with surveillance access control security system.
- Authorized e& enterprise staff/personnel 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/enclosures for routine site health check/audit purposes 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 adhere to rules of conduct and safety signage at the entrance of the Data Center equipment room.
- Data Center ceilings are fitted with FM200/Inergen/argon/Novec 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.

- In case of emergency, contact the onsite Data Center staff immediately.
- Smoking is not permitted at any time in the Data Center building.
- All kinds of food, beverages, Cigar lighters, and any kind of hazardous materials 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.
- Manual Fire distinguisher being distributed on Data Center floor in designated area for manual intervention

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 90 Days for All Data Centers, 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 E& enterprise 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 / any other media 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 anywhere else within the Data Center. E& enterprise 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 to all vendors/customers visiting the Data center.
- No CCTV footage will be allowed to be watched/reviewed by Customers as it's a 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

- Only the persons listed on the approved ticket created by the customer will be granted access to the Customer's contracted area. The Customer remains responsible for their activities.
- The Persons identified in the authorized contact list only will be allowed to access the Datacenter without a ticket in case of any emergency situation.
- Customer must carry official/valid documents* to obtain approval from onsite Data Center support team for created access request prior to entering the DC premises for planned/unplanned access.

  *Official document(s) to perform any onsite activity.
  - Foreigners: Passport & Valid Work / Mission Visa issued by UAE Government
  - GCC nationals: GCC national ID
  - UAE Residents/Citizens: Emirates ID

  - Valid UAE visit visa / GCC residency Visa holder can be used only for meetings and site visits.
- All Customer's staff/vendors/contractors 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. E& enterprise Data Centers have a restricted access policy, customers have to adhere to E& enterprise 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 E& enterprise premises
- E& enterprise Data Center requires a written submission of customer authorized list upon signing Hosting agreement with e& enterprise (for who has permitted to access his hosted equipment within E& enterprise 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 an updated authorized list, any modification (additions/deletions) of the list should be updated in the authorized contact list form and addressed to E& enterprise Data Center Team through ticket.
- Data Center shall not hold any responsibility for the activities carried out by individuals whose authorization are revoked and not updated to Data Center by the customer. Customer should update/ reconfirm his authorization list on routine/regular 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 E& enterprise Data Center Support team via the support portal ticketing system, prior to their visit.

5.2 Data Center Entry/Escorting Procedure

- Customer and their authorized representatives may access the Data Center facility 24/7 upon logging a ticket through the support portal.
- Customer should provide Data Center staff with information about the 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 team through the support portal (https:// managedservices.etisalat.ae).
- If the customer is facing any login issues on the support portal, access requests can be sent through authorized contact email to the Data Center team email id: (support@dc.etisalat.ae), and for Smart Hub customers access requests to be sent to (smarthub@dc.etisalat.ae). Then, Data Center team will raise the access ticket and will reply to the customer's mail with #REQ/INC reference number, the customer may contact the Data Center team for follow-up toll-free number 8004181 (within UAE) or +971 8004181 (overseas customer).
- During the provisioning/ installation stage for new customers, access requests can be raised for one week or more subject to approval.
- During the provisioning/ installation stage, access request can accommodate a maximum of 10 visitors/ personnel per activity/visit. If more visitors are required then approval to be obtained from the Data Center team with proper justification.
- For operational Customers, access request are to be raised for each day (each ticket valid for one day). However, access can be extended for a maximum of one week upon Support team approval.
- For an operational customer, each access request can accommodate a maximum of 5 visitors/personnel per activity/visit. If more visitors are required then approval to be obtained from the

Data Center team with proper justification.

- In case of emergency, authorized persons will be granted access, and the Data Center team will assist them in case of an account login issue onsite team will open a ticket on their behalf upon end-user confirmation.
- Cabinets and cage keys shall be held with the 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.
- Upon entering the Data Center, the following shall be available depending on your visit purpose:
    - Valid Service Desk ID i.e., #REQ/INC******
    - Possess and exhibit at request, Via government-issued document,
        - Foreigners: Passport & Valid Work / Mission Visa issued by UAE Government
        - GCC nationals: GCC national ID
        - UAE Residents/Citizens: Emirates ID
        - Valid UAE visit visa / GCC residency Visa holder can be used only for meetings and site visits.
    - 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 during the week working days between the hours of 8 AM and 2 PM UAE local time. However, subjected to approval, delivery of shipment may extend to 24x7.
- In case of an emergency an approval must be obtain from Data Center Team.
- If delivery is approved, Customers shall provide at least 48 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 any 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, in case of installation delay, customers should ensure that to take uninstalled items back while leaving the premises.
- 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 bay 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 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 Data center Team.
- 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 Data center Team 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. DC Onsite Team 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 the DC Storeroom 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 the equipment's/items that belong 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 the Data the enter team.
- 48 hours notification is required to remove/replace/add any equipment, **in case of an emergency** need to obtain 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, the customary may be allowed, to deliver, install & configure his devices during non-business hours subjected to prior notification and approval from back-office team on valid register REQ/INC 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 hold 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 E& enterprise Data Center prior to leaving the premises. E& enterprise will be holding 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, E& enterprise 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 their Equipment conforms to the current Data Center standards and is in good operational condition, all equipment's shall have redundant power supplies or Powered through ATS/STS. Installation of Customer Equipment shall at least comply with:
    - E& enterprise 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 E& enterprise Data Center.

- Un-racked equipment is strictly prohibited in or outside the contracted area.
- Customers with Cage subscription must label all their Equipment, 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 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 planned in advance or on an appointment basis with onsite Data Center team.
- Fillers/Blanking panels must be installed in the free U's of the cabinet in order to maintain the airflow. For Cabinets owned by the Customer the blanking panels also need to be arranged by the customer.
- In case the customer's owned cabinet, perforated doors must be installed in order to maintain airflow with in the Data Center white space.
- Authorized E& enterprise staff/personnel reserves the right to take photos inside customer's cage/enclosure/rack whenever the customer requested for his equipment details, auditor for audit purposes, and for Operational requirements such as incidents and violations.

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 the Customer's attention.
- Customers must not conduct any activity that may adversely affect the provision of e& enterprise 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 E& enterprise 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 the healthy environment of the E& enterprise 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.
- 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 rack's structure is not allowed for hosting IT equipment within e& enterprise hosting Data Center as it's 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 air 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 E& enterprise hosting guidelines

- The height of the rack will determine how many rack spaces (Us) 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 is 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 un-used RU spaces must be filled.
- Customer must extend earthing (grounding) to all his cabinets/Racks (Mandatory) to a designated structured local earthing bars/strips which are linked back to the main building MET (Main Earthing Terminal), in case of any assistance please refer to onsite Data Center team.
- All Metallic Rack/cabinet components, including the roof, doors, rails, side panels, chassis, and frame should be grounded for personnel safety from electrical short circuit and to avoid potential damage of equipment.
- 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.

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 ASHARE 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.
- In order to enhance customer experience and improving business continuity Customers should bring their all-IT equipment/devices equipped with dual/redundant power supply; in case of single power supply device customer should bring **automatic transfer (ATS)** switch.

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.
- Arrange patch bays to minimize patch cable lengths and to simplify cable management.
- Data Center Cable management separated pathways for each media types power and communication cables must be placed in separate pathways or separated by a physical barrier, adequate space must be provided with cable trays for better cable management which provides benefits to improve administration, and minimize damage to smaller diameter cables.
- Cable trays must be installed in multiple layers and it should be separated from ceiling.

9.0 Technical Limitation

Weight: Floor load should not exceed approved distributed load.

Power: Power configurations should be available upon request and where agreed by Data Center Team. Hosting packages cabinet socket types are 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 13A In case of 16 Amps PDU and 26A in case of 32 Amps PDU 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 or space in the cabinet/cage, 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 perm^2). 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 ASHARE 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.
- Customers are not allowed to drag equipment over the raised floor, they need to 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.
- e& enterprise 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.
- Authorized E& enterprise staff/personnel is permitted to take photos inside customer's cage/enclosure/rack whenever the customer requested for his equipment details, auditor for audit purpose, and for Operational requirements such as incidents and violations.
- Customer is not permitted to approach, handle, use, inspect or examine any equipment, cabinets, cage space, other than their cabinets.
- Customer is not allowed to conduct any practices that could be harmful for personnel healthy/safety or danger/hazardous of electrical short.
- Customer is not permitted for misusing the facility and conducting any activities which could lead for physical or logical security breach or attempt to tap other customer setup or attempt to bypass network or attempt for internet hacking.

- Misconduct related to any reported unauthorized activities that contradicts with the government laws, and/or other misleading, criminal or unlawful purposes found within customer areas will be suspended immediately.
- Major abuse of the service which may cause severe damage to E& enterprise physical infrastructure /property assets/network infrastructure or may cause business services interruptions/major-outages any such activities will lead to suspend the customer account immediately.
- E& enterprise reserves the right, at all times, to remove, change, or otherwise terminate the operation of the Customer equipment installed in Customer's space without notice if E& enterprise deems, in its sole discretion, to protect the personnel's safety or facilities or services from severe damage or injury of any kind, or due to any abusive behavior that harass, threaten, harm or defame by customer employee/vendors

11.0 Emergency Response Procedure

This Emergency Response Plan has been designed to provide vital information and guidance to Hosting customer and E& enterprise Internal Staff in the event of a major emergency on Data Center (DC) campus. The below listed procedures are intended to be used as general guidelines and does not cover every conceivable situation.

While it is not practical to suggest that these procedures will be followed verbatim during any actual emergency, they will provide vital information on how staff, customers and emergency response team can respond to such situations.

11.1 Purpose and Goal

The main goal of the Emergency Response Plan is the preservation of life, protection of property, and the continuity of DC operations. Other objectives include but are not limited to:

- Delegation of responsibility to emergency personnel.
- Coordination of emergency operations with external agencies such as the Fire Department, and other applicable agencies and organizations.

11.2 Emergency Classification

LEVEL OF EMERGENCY	DESCRIPTION
Level 1	An emergency has occurred and can be controlled by onsite DC & security teams.
Level 2	An emergency has occurred. However, the situation is not under control but is confined within facility premised. The emergency is confined to a small area or to a fixed site and does not posed a threat of spreading to a larger area or off-site. The onsite DC & security teams shall take the necessary response for controlling the situation with liaise of Corporate HSE and DC High Management.
Level 3	An emergency has occurred where the situation is not under control and protective action may be necessary to protect the surrounding or offsite area. A site area emergency involves events in process or which have occurred that result in actual or likely major failures of DC facility safety functions. Onsite DC & security together with Civil Defense, Police and other Agencies shall take the necessary response for

	controlling the situation. As well, as DC Manager shall inform and liaise with Corporate HSE and DC Higher Management respect to the existence situation.

11.3 Identification and Deployment Emergency Response Plan

- Types of events that could cause accidental or uncontrolled release of the substance (fire, equipment failure, impact, operator error, other abnormal operating conditions, etc.);
- The nature and severity of environmental impacts that could be caused by an accident or uncontrolled release;
- Availability of methods and measures to prevent or reduce HSE impacts and hazards that would result from the accident.
- As appropriate, emergency response plans may include such elements as:
- Training
- of personnel designated Fire warden (Name is available on each DC floor) for coordinating and carrying out emergency response actions;
- Personal protection equipment;
- Evacuation plans and procedures.
- Identification and communication with outside assistance and other resources (police, fire department, hospitals, special emergency response services, etc.);
- Notification of appropriate authorities and organizations; and so forth.

11.4 Incident Management Reporting

This plan is designed to minimize operational and financial impacts of such a disaster, and will be activated when a local Incident Manager (or, in his/her absence, one of his/her alternates) determines that a disaster has occurred. Specific details on incident response and subsequent business recovery actions and activities are included within the respective local recovery team plans.

Monitoring tools Data Center Infrastructure Management (DCIM) software including Building Management Systems (BMS) can be very helpful in simplifying and automating incident notification (and reporting) assuming infrastructure systems are metered, instrumented, and communicating with the software, of course. Alarm thresholds and notification policies can be centrally configured and managed.

Incident reporting

A standardized template should be used to report all incidents (sample enclosed). This helps ensure all of the relevant information is gathered every time. The report should contain the following information. (Please Refer to Annex 12.6 for incident Report Sample Report for more clarifications).

Report information

- Report title
- Date and time of Incident Start
- Date and time of Incident Resolved

Site information

- Site identifier
- Site point of contact (POC)

Incident overview

- Brief description of incident
- Location affected by incident (e.g. generator bay, UPS room, or entire facility)
- Equipment involved
- Affected Customer details

- Incident attributes

Incident details

- Time/date of incident and duration
- Who discovered it
- Who was present
- Describe initial response actions
- Root Cause of the incident
- Is the problem occurred earlier
- Who was notified and when
- How the situation was stabilized or resolved

Action items

- Specific task(s) to correct or provide additional information about the incident
- (E.g., ordering a part, calling a vendor, long term monitoring of the issue).
- Expected or required completion date for the task.

Recommendations/Remarks

- Any recommended action or actions that should be taken to prevent future incidents.

11.5 Emergency Equipment Monitoring & Inspection

- Onsite DC Team shall ensure that appropriate emergency equipment is provided, deployed and easily accessible in strategic areas of the DC premises, where potential HSE emergency and associated risks could potentially occur.
- Onsite team to ensure that vender/ customer/ internal staff must obtain (work permit) from HSE team prior to any activity, installation, dismantling, drilling, and/or impacting white space infrastructure.
- Emergency equipment(s) shall cover all but not limited to the following:
    - Fire Extinguishers
    - Fire Alarms / Fire Hose
    - First Aid Kit / Spills Kit (in the event of chemical oil spills)
    - Emergency Lights

11.6 Recommended Procedures in Emergency

This section entails a list of recommended procedures for some types of emergencies. These procedures may be followed in sequence unless conditions dictate otherwise. (Please Refer to Annex 12.7)

11.7 Evacuation Routes

Evacuation route maps have been posted throughout campus in many strategic locations. The following information is marked on evacuation maps:

- Emergency exits
- Primary and secondary evacuation routes
- Locations of fire extinguishers
- Fire alarm pull stations' location
- Assembly points

12.0 Annex:

12.1 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://managedservices.etisalat.ae for any kind of visits and get the approval before visiting the Data Center.
- All visitors are registered while 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.

12.2 Authorization of Access – Setting up Access – Authorization list

- Only main authorized contact person is 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 contact should be available/reached 24 x 7 hours to validate access requests and to provide any Missing information.
- 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 Team. Data Center aims to make any change within 2 working day of having received notice of such change.

12.3 Revoking Access

- EMERGENCY: In case of revoking Access or Authorization privileges, it would be 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
- Etisalat DC may refuse entry to, or require the immediate departure of, any individual who:
- Fails to provide proof of valid documents (Passport, Visa, GCC national ID and Emirates ID etc.)
- fails to comply with this Data Center Use Policy,
- Fails to comply with any of Etisalat DC other policies, procedures and requirements after being advised of them.

12.4 Conduct Guidelines

- Customers may not misuse or abuse any Etisalat DC 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.

12.5 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.

12.6 DC Incident Report:

Data Center Incident Report

- Site Name: XXXX-DC
- Report Date: XX/02/20XX
- Service Type: Managed Hosting DC
- Time: XX: XX PM – XX: XX PM (XX minutes)
- Description: XXXX
- Target Customer: XXXX
- Ticket: INC000000XXXXX
- Contact Information: XX name of staff only XX

Incident Background and Executive summary:

- Please mention brief of incident and background information.

Event timeline:

- DC team to mention here details of timeline while working or handing the incidents.

Root Cause Analysis & Reason for failure & Observation /5 why's: (if applicable) –

Reason/Root cause for failure to be mentioned here and along with that detailed RCA report including 5 whys concept (who observed it, how many customers affected, why this problem happen, when problem first noticed, has the problem occurred previously etc.) details to be mention here.

Actions taken for Incident Resolution & Recommendations: (if applicable)

We recommend you to…Based on Data Center standard industry practices…. also include resolution & recommendation prior to closing the incident.

Closure & Action Tracking / Remarks: (if applicable)

Based on above comments/justification from concern section; ….

Regards,

Data Center Team | Etisalat

12.7 Recommended Evacuation Procedure:

Earthquake:

- Stay calm and await instructions from the Emergency Coordinator or the designated official.
- Keep away from overhead fixtures, windows, filing cabinets, and electrical power.
- Assist people with disabilities in finding a safe place.
- Evacuate as instructed by the Emergency Coordinator and/or the designated official.

Flood:

If indoors:

- Be ready to evacuate as directed by the Emergency Coordinator and/or the designated official.
- Follow the recommended primary or secondary evacuation routes.

If outdoors:

- Climb to high ground and stay there.
- Avoid walking or driving through floodwater.
- If car stalls, abandon it immediately and climb to a higher ground.

Hurricane:

- The nature of a hurricane provides for more warning than other natural and weather disasters. A hurricane watch issued when a hurricane becomes a threat to a coastal area. A hurricane warning is issued when hurricane winds of 74 mph / 120 kmh or higher, or a combination of dangerously high water and rough seas, are expected in the area within 24 hours.

Once a hurricane watch has been issued:

- Stay calm and await instructions from the Emergency Coordinator or the designated official.
- Moor any boats securely, or move to a safe place if time allows.
- Continue to monitor local TV and radio stations for instructions.
- Move early out of low-lying areas or from the coast, at the request of officials.
- If you are on high ground away from the coast and plan to stay, secure the building, move all loose items indoors and boarding up windows and openings.
- Collect drinking water in appropriate containers.

Once a hurricane warning has been issued:

- Be ready to evacuate as directed by the Emergency Coordinator and/or the designated official.
- Leave areas that might be affected by storm tide or stream flooding.

During a hurricane:

- Remain indoors and consider the following:
- -Small interior rooms on the lowest floor and without windows,
- - Hallways on the lowest floor away from doors and windows, and Rooms constructed with reinforced concrete, brick, or block with no windows.

Tornado:

When sirens issue a warning or other means, seek inside shelter. Consider the following:

- Small interior rooms on the lowest floor and without windows,
- Hallways on the lowest floor away from doors and windows,
- Rooms constructed with reinforced concrete, brick, or block with no windows.
- Stay away from outside walls and windows.
- Use arms to protect head and neck.
- Remain sheltered until the tornado threat is announced to be over.

12.7.1 Fire: General Fire Safety Precautions:

- If you suspect someone is trapped inside a building during a fire, notify the fire fighters on scene or Safety personnel. Do not re-enter a burning building.
- As soon as possible, call 997
- If you are trapped in a fire, attempt to leave the building. Cover your nose and mouth with a cloth or T-shirt. If it is not possible to exit through a door, find another exit such as a window. If possible, place wet towels or clothing in the cracks around the door. Jumping from a window is only to be considered when you are in immediate danger.
- If you exit through a door, stay low to the floor but do so with caution. Use a wet towel or blanket to protect yourself from flames and smoke.
- Many fires are of electrical origin. Check for frayed cords, broken plugs, and avoid using too many appliances in one circuit.
- Be familiar with emergency exits inside your building as well as the location of fire extinguishers.
- Move away from the building to your pre-determined evacuation assembly area.
- A campus Emergency Command Centre may be set up near the emergency site. Keep clear of the Command Centre unless you have official business there.

- Do not return to an evacuated building unless told to do so by BMS or onsite operations staff.

Fire extinguishers are located throughout campus in many strategic locations. Learn to identify the extinguishers and find out where they are located in your area. In the event of a small fire that would not put your safety at risk, utilize the fire extinguisher if you are capable of doing so. If you decide to use a fire extinguisher, follow the instructions listed below on how to operate a fire extinguisher.

Learn how to **P. A. S. S.**

PULL – the pin or ring, or release the lock latch.

AIM – the extinguisher nozzle at the base of the fire.

SQUEEZE – or press the handle.

SWEEP – from side to side slowly at the base of the fire until it goes out

12.7.2 Hazardous Leak or Spill

Take steps to protect all chemical containers and gas cylinders in the event of a violent shake from an earthquake.

- Any serious chemical spill should be reported to Facilities Services and Safety/HSE personnel immediately.
- Depending on the severity of the spill, be prepared to evacuate the building.
- Stay upwind and upstream of the spill.
- In the event of a large off DC campus spill, evacuation of the campus may be necessary. Be prepared to cooperate with Civil defense/Emergency services legal authority officials.

12.7.3 Power Outage

In the occurrence of any such outage in office areas, Data Center bays, or hot seat areas; the emergency team is prepared to do the following task to help others:

No	Action Taken	Comments
1	Determine extent of outage, if backup power systems engaged	Contact operations team via cell phones, check power supplies, use rechargeable flashlights to move around safely
2	Determine if staff need to evacuate	Meet with Operations team e.g.DCS/FM/BMS/onsite security team and follow the instructions
3	Assess potential damage to firm; ensure that critical data is backed up and protected	Refer to above comments
4	Contact senior management	Advise on initial situation
5	Contact utility company	Contact via cell phone, unless PBX system is operational, arrange to have emergency crew dispatched

6	Identify cause of outage, launch remediation efforts	Work with utility company electricians, others
7	Assess when Data Center operations can resume	Meet with Operations team e.g.onsite DC/FM/BMS/onsite security team
8	Contact senior management, send regular updates on progress.	Advice on response, remediation and ongoing efforts post outage.

12.7.4 Evacuation Procedures: General Evacuation Procedures

Building evacuation will occur via one of the following mechanisms:

- When a building evacuation alarm (fire alarm) is sounded.
- Upon notification by a Safety officer, or by a floor/building coordinator.
- When a signal to evacuate the building is given:
- If possible, take your personal belongings with you.
- Walk quickly to the nearest marked exit or stairwell.
- Do not use the elevators.
- Assist people with disabilities or special needs to exit the building.
- Once outside the building, move to your designated evacuation area.
- Stay at least 200-300 feet away from any affected buildings or structures.
- Keep streets and walkways and fire zones clear for responding emergency vehicles and personnel.
- DO NOT return to an evacuated building unless directed to do so by a Safety Officer, a building/floor coordinator, or other emergency response personnel.

IMPORTANT: Under no circumstances should a customer, client or any member of the DC unilaterally decide to ignore a fire alarm, fire drill, or a request for evacuation.

12.7.5 Disabled Person Evacuation

This section provides a general guideline of evacuation procedures for persons with disabilities during major emergencies. Individuals with disabilities must identify their primary and secondary evacuation routes. Onsite DC Team and customers are encouraged to assist any disabled or injured persons to evacuate a building or structure.

a) Evacuation of MOBILITY-IMPAIRED Persons – WHEELCHAIR

In most multilevel buildings, people will need to use stairways to exit a building during a major emergency. Elevators are not recommended because they have been shown to be unsafe in an emergency. For persons in wheelchairs located on the first floor, use building exits to the outside ground level. For disabled individuals on upper floors, it is not safe to attempt to move a wheelchair down a stairwell. Evacuation options include:

Person Cradle Carry

- Make sure the stairwell is clear.
- The two helpers stand on either side of the individual.
- Reach under the individual and lift them out in a cradle.
- Helpers should control the descent by walking slowly and cautiously.
- NEVER LEAVE A WHEELCHAIR IN A STAIRWELL.

b) Evacuation of MOBILITY IMPAIRED Persons - NON-WHEELCHAIR

Persons with mobility impairments who are able to walk independently should be able to negotiate stairs in an emergency with minor assistance. The individual should wait until the heavy traffic has cleared on the stairwell before attempting to exit.

c) Evacuation of HEARING-IMPAIRED Persons

Some buildings on campus are equipped with fire alarm strobe lights; however, many are not. Persons with hearing impairments may not hear audio emergency alarms and will need to be alerted to emergencies by other building occupants.

d) Evacuation of VISUALLY IMPAIRED Persons

Most people with a visual impairment will be familiar with their immediate surroundings and frequently traveled routes. Since the emergency evacuation route may be different from the commonly traveled route, persons who are visually impaired may need assistance in evacuating. The assistant should offer his/her elbow to the individual with a visual impairment and guide him or her through the evacuation route. During the evacuation, the assistant should communicate as necessary to ensure safe evacuation.

12.7.6 Emergency Contact Number

Customer may contact Data Center team on toll free number 8004181 (within UAE) or +971 8004181 (overseas customer) at 24/7/365 for any further assistance.

Emergency services	
Police emergency	999
Police non-emergency	901
Ambulance	998 or 999
Facilities Protection services and maritime facilities	996
Fire brigade	997 or 999
Traffic and transport	
Roads & Transport Authority Dubai	800 90 90
Abu Dhabi Traffic Patrol	600 533 333
Report traffic offences	800 4353
Traffic violations and e-pay	800 7777
Government institutions	
Abu Dhabi Municipality	800 22220
Dubai Municipality	800 4567
Emirates ID Authority	600 530 003
Emirates Post	600 599 999
Ministry of Education	800 51115
Ministry of Health	800 11111
Ministry of Interior	800 5000
Ministry of Justice	800 333 333
Ministry of Labor	800 665
Utilities	
Abu Dhabi Distribution Company	800 2332
Federal Electricity & Water Authority	800 3392
Al Ain Distribution Company	800 9008
Dubai Electricity & Water Authority	991
Sharjah Electricity Emergency	06 565 7575

Sharjah Gas Emergency	800 6333
Sharjah Water Emergency	992
Crime reporting	
Al Ameen (crime reporting)	800 4888
Anti-narcotics department	800 400 400
Human trafficking	800 5005
Victim communication	800 243

12.7.7 Access protocol during pandemic

During any pandemic situation the access to the Etisalat datacenters will be based on the U.A.E Government and TDRA authority's instruction and guidelines includes preventive and reactive measures, which are implemented considering the risk situation.

Covid access protocol

In line with government guidelines, the below protocols need to be followed while accessing any Etisalat datacenters During Covid,

- Access to Etisalat buildings and Data Centers will be limited to employees, contractors and customers with valid Green Pass in ALHOSN Mobile App or with an approved exemption from UAE health authorities which has to be shown to Building Security Guards or whenever requested in the facility.
- If you do not have Green Pass in ALHOSN Mobile App , you can activate your access permission in the short term, so long as you can provide a recent negative PCR result (valid for 2 days from result date).Overseas visitors must provide valid PCR result /medical report / attendance from authorized medical center in the UAE.
- Thermal scanning machines/handheld devices in Etisalat premises have been installed to detect high body temperatures. Please allow security to check your temperature if required
- If sickness symptoms observed on DC visitors, he/she will not be permitted inside Etisalat Data Center.
- Visitors to DC must take care of their own protection (wear their own Mask and Gloves), any visitor will not be authorized to enter Etisalat premises without wearing a mask.
- Follow the guidelines labels on the entrance of each elevator, floor, and pantry regarding maximum number of employees
- Avoid handshaking, use other non-contact methods of greeting.
- Practice physical distancing by avoiding gatherings and maintaining distance (approximately 2 meters) from others.