

NTT Com Asia Limited
(hereinafter referred to as the “Company”)
Hong Kong Financial Data Center (FDC)
Data Center Policy (the “Policy”)

1. DEFINITIONS

- 1.1 Except for the following capitalized terms which have the same meanings as defined in the Nexcenter Service Terminology, all other capitalized terms used in this Special Conditions shall have the same meanings as defined in the General Conditions.

Data Center(s)

Authorized Visitors

Colocation Space

Cage

Rack

Customer Rack

The Hong Kong Financial Data Center is a secure facility and any unauthorized personnel are prohibited to enter the Data Center premises. The Customer and its Authorized Visitors can enter and access the designated Data Center zone for equipment placement and other services subscribed (“Colocation Space”) with the submission of duly executed Customer Authorized Access Form or registered in Access Management System. Customer Representatives are restricted to access other zone within the Data Center except for the Company’s permission. All access to Data Center must be accompanied by the Authorized Visitors at all times except stated in access request in Access Management System.

For Customer Authorized Access Form, it is the Customer’s responsibility to ensure that all changes of the Authorized Visitors are notified to the Company in a timely manner with the submission of an updated Customer Authorized Access Form.

For Access Management System, it is the Customer’s responsibility to update all the changes of the Authorized Visitors in Access Management System. It is also the Customer’s responsibility to procure registered guest and authorized person to exit Data Center before expiration of the reserved access time period and access profile time period respectively. Upon the expiration of the reserve access time period and access profile time period, the registered guest and authorized person will have no right to remain in Data Center.

This printed copy may not be the latest version. Please verify against the electronic version in SharePoint prior to use.

For avoidance of doubt, Customer understands and agrees that failure to exit the Data Center after the expiration of the reserved time period or access profile time period (as the case may be) will constitute a violation of this Data Center Policy and the Company reserves its right to take immediate actions to request the registered guest and/or the authorized person to leave the Data Center without any liability on the Company's part.

Customer is fully responsible for all acts or omissions of its Authorized Visitors, accompanying persons, associated companies and all such acts or omissions will be attributed to Customer for all purposes, including for the purposes of determining whether Customer has breached this Policy. Without limiting the foregoing, Customer must ensure that its Authorized Visitors, accompanying persons or associated companies, do not take any actions that Customer is prohibited from taking under this Policy.

2. USE OF DATA CENTER FACILITY

2.1 Conduct at Data Center

- 2.1.1 Customer and its Authorized Visitors agree to adhere to and abide by all security and safety measures established by the Company. Customer and its Authorized Visitors shall not be involved in any of the following acts:
- (a) misuse or abuse any of the Company's property or equipment or third party equipment;
 - (b) make any unauthorized use of or interfere with any property or equipment of any other customer;
 - (c) harass any individual, including the Company personnel and Authorized Visitors of other customers;
 - (d) engage in any activity that is in violation of the laws or aids or assists any criminal activity while in the Data Center or in connection with the Data Center Services;
 - (e) behavior that will infringe the privacy of the Company personnel and other customers;
 - (f) use of any photographic, video, film or such other device that produces, reproduces, retains or transmits images within the Data Center and the Colocation Space; and
 - (g) wandering around inside the Data Center without accompanying by the Company representative.
 - (h) open any raised floor panels unless the customer have notified the data center operator
 - (i) operate or touch any button, switch and knob on the data center's facilities or the equipment of which do not belong to the customer;
 - (j) do drilling or swirling which may cause false alarms or trigger the Highly Sensitive Smoke Detection System;
 - (k) climb any Cages, ladders, Racks, or support structures;
 - (l) leave unattended objects outside the subscribed racks inside the colocation room
 - (m) wear attire deemed inappropriate (e.g. must wear a shirt, shoes, and pants/dress/skirt; no profanity or obscenity on clothing; etc.
- 2.1.2 Customer and its Authorized Visitors are required to observe our Acceptable Use Policy while accessing internet within our Data Center. Copy of the Acceptable Use Policy can be found in our Company website.

This printed copy may not be the latest version. Please verify against the electronic version in SharePoint prior to use.

2.2 Prohibited Items

2.2.1 Customer and its Authorized Visitors shall keep each Colocation Space clean, free and clear of debris and refuse at all times.

2.2.2 Customer shall not, except as otherwise agreed in writing by the Company, (i) place any computer hardware or other equipment in the Colocation Space that has not been identified by the Company; (ii) store any other combustible materials of any kind in the Colocation Space; and (iii) bring any of the following prohibited materials (“Prohibited Materials”) into Data Center. Prohibited Materials shall include, but not limited to, the following and any similar items:

- Food and drink
- Tobacco products
- Explosives and weapons
- Flammable materials
- Chemicals, solvents, cleaners or paints
- Hazardous materials
- Inflammables
- Pallets
- Water rich items (umbrella etc.)
- Alcohol, illegal drugs and other intoxicants
- Electro-magnetic devices, which could unreasonably interfere with computer and telecommunications equipment
- Radioactive materials
- Photographic or recording equipment of any kind (other than tape back-up equipment)
- Creatures (pet, plant, etc.)
- Unauthorized Power Supply alteration or non verified power usage
- Climate-control device
- Objects with a bad odor,
- Objects that rots or transforms very easily
- Liquid substances (beverage, etc.)
- Magnetic devices
- Any other items deemed inappropriate at the Company’s sole discretion

2.2.3 Customer is required to leave the belongings in a locker located in the security counter and only brings the required items to the Colocation Space. Customer’s *belongings* may be examined by the Company

This printed copy may not be the latest version. Please verify against the electronic version in SharePoint prior to use.

representative before Customer enters the Colocation Space. Customer's visit may be rejected if the Company regards Customer to be uncooperative.

- 2.2.4 The Company shall not be responsible for any kind of loss within the Data Center so Customer is advised not to bring valuable belongings to the Data Center.

2.3 POWER

- 2.3.1 Each of the Company's standard rack and/or cabinet is provisioned with dual power feeds according to the Company's predefined power capacity. The maximum number of power sockets allowed in a standard rack or cabinet is specified in the customer order form. Upon Customer's request, the Company may, at its discretion, provide racks and cabinets with higher power rating configurations, or with more power feeds and power sockets, subject to additional charges quoted. The Customer could only use those power sockets as assigned by the Company. At no time is the Customer allowed to install his/her own power bar, or power more electrical devices than the number of sockets as agreed by the Company.
- 2.3.2 The power configuration of each Customer Rack must be prior approved by the Company in writing and the Customer must comply with the laws, rules and regulations, codes and directives where applicable. It is the Customer's sole responsibility to ensure that:
- (a) they have ordered enough number of power sockets to power each device; and
 - (b) the power provided as agreed by the Company is sufficient to power the devices for regular use.
 - (c) they do not install additional power extension cord within the rack.
- 2.3.3 The Company may independently inspect the power configuration of any of the Customer Racks at any time.
- 2.3.4 The Company may, direct Customer (i) to alter the power configuration of Customer Equipment; (ii) to disconnect power supply to the Customer Equipment; or (iii) require Customer to remove from any equipment, forthwith, if the Company, at its sole discretion, deems that the continued operation of Customer Equipment:
- (a) causes a threat to safety (including any risk of fire or other hazard) to the operations of the Company's Data Center or the Data Center property;
 - (b) unreasonably interferes with the operations of the Company, any other customer or any other person or otherwise utilizing any portion of the Data Center or the Data Center property; or

This printed copy may not be the latest version. Please verify against the electronic version in SharePoint prior to use.

- (c) is not installed in accordance with standard industry practice; and/or
- (d) is consuming or has consumed excessive power.

2.3.5 The Company reserves the right to disconnect any unauthorized power connection made by Customers without notice.

2.4 EQUIPMENT AND CONNECTIONS

Customer shall ensure that:

- (a) all of the Customer Equipment must be installed, operated, configured and run at all times in compliance with the manufacturer's specifications and the applicable safety codes, including power outlet, power consumption and clearance requirements where the industry practice applies;
- (b) all of the Customer Equipment must be unpacked and configured in staging rooms before putting into Customer Racks;
- (c) provide the Company with no less than two (2) working days prior written notice if Customer intends to move-out any Customer Equipment;
- (d) all Customer Equipment must be put within the Customer Racks, and they must be either rack-mounted, or be put on the Company's provided fixed partitions or any other area designated by the Company. Any of Customer Equipment that is too large or heavy for a rack or cabinet, including but not limited to large servers, will be securely fixed directly to the floor by the Company. The Company may charge Customer for performing such service;
- (e) none of Customer Equipment is stacked or resting on the equipment of any other customer or third-party;
- (f) all of the cables and wiring in Customer Racks are neatly wrapped and tied together (if a customer fails to do so, the Company may in its sole option neatly wrap and tie such wires and cables, and the Company reserves the right to charge the customer for performing such service); and
- (g) all equipment is arranged in such a way that there is ample space for good ventilation within the Customer Racks.

IF CUSTOMER BREACHES ANY OF THE TERMS MENTIONED IN THIS POLICY, THE COMPANY RESERVES THE RIGHTS TO SUSPEND OR TO DISCONNECT THE SERVICES PARTLY OR WHOLLY, OR TERMINATE THE AGREEMENT AT ITS OWN DISCRETION WITHOUT INCURRING ANY LIABILITIES OR OBLIGATIONS WHATSOEVER.

MODIFICATION OF RULES AND REGULATIONS

The Company may change this Policy at any time and from time to time and the revised Policy shall be posted at <https://hello.global.ntt/en-us/legal/privacy-statement> Customer is required to review the Company's website regularly to keep yourself informed of the most current version of this Policy at all times.

This printed copy may not be the latest version. Please verify against the electronic version in SharePoint prior to use.