

Qu Data Center Customer User Policy (“Policy”)

THE TERMS OF THIS POLICY are in addition to, and operate together with *Customer Orientation Guide* applicable to each specific Data Centre facility operated by Qu. A Customer that contravenes the requirements of this Policy may, at the reasonable discretion of Qu, be considered to have materially breached the terms of their Service agreement with Qu; and therefore Qu may avail itself to all remedies under such agreement and at law.

Access to the Data Centre

All persons requesting access into a Qu Data Centre (“**Visitor/s**”) must be positively identified. This process requires Visitors to (a) show a valid (unexpired) Canadian government issued photographic identification to Security Operations, such as a valid provincial driver’s license, provincial health card or Canadian passport; and (b) complete the ID Badge Access Request Form.. After such identification and confirmation of the Visitor’s authorization to attend the Data Centre, Qu will issue the Visitor an ID badges (“**ID Badge/s**”); this ID Badge permits the Visitor to access certain controlled areas of Data Centre facilities.

All Visitors must wear an ID Badge (temporary or permanent) when attend the Data Centre. All ID Badges are the property of Qu and must be returned upon request. No modifications or additions should be made that interfere with the visibility, clarity, or use of the ID Badge. ID Badges must be worn on by each Visitor in a manner that is openly visible at all times. ID Badges are issued to an authorized Visitor and must not be shared or used by any other person. The sharing of badges or PINs between Visitors for any purpose whatsoever is strictly prohibited. The Data Centre access control system will automatically deactivate a Visitor’s ID Badge after sixty (60) days of non-use.

Data Centre Contact List

In order to maintain the security of the Data Centers, Customers are required to provide Qu with an accurate information of all employees, representatives and contractors that require access to the Data Centers and Customer cages (each an “**Authorized Personnel**”). Qu’s Security Operations relies on Customer’s information about their Authorized Personnel to grant Visitors with access to the Data Centre facilities. Failure of the Customer to accurately notify Qu in a timely manner about all its Authorized Personnel will result in the Customer’s Visitors being denied access to enter the Data Centre Facilities. The Customer may update Qu about its Authorized Personnel information by contacting its Qu designated Account Representative or Qu’s Service desk.

Customer Access

The Customer is responsible for the conduct of its Authorized Personnel at the Data Centre facilities, including their compliance with this Policy and the reasonable verbal direction of Data Centre staff.

Customer and its Authorized Personnel may only access that portion of a Data Centre made available by Qu to Customer for the placement of Customer's equipment and use of the Data Centre Services (the “**Customer**

Area”), and common areas of the Data Centre (e.g., entryways and bathrooms) unless otherwise approved and accompanied by an authorized Qu representative..

Customer shall cause its Authorized Representatives to comply with the terms of this Policy, including the following:

- Shall not permit any unauthorized persons to access the Data Centre (e.g., by “tailgating” or other means);
- Shall not use, touch, inspect or otherwise interface with any Qu or third party property or equipment;
- Shall not harass or interfere with the activities of any individual within the Data Center, including any employees or representatives of Qu or other customers;
- Shall not engage conduct that is contrary to the terms of this Policy or that is unlawful.;
- Shall not store any computer hardware or other equipment in the Customer Area that is not used by the Customer in connection with the Qu’s provision of Services for the Customer; and
- Shall not engage in any construction activity that changes or alterations to the interior or exterior of the Data Centre or the Customer Area.

Data Centre Tour Policy

A Customer tour group of six (6) or more Visitors must follow these Data Centre Tour Rules. For tours, the ratio of visitors to Customer’s Authorized Personnel is 10:1. Tours of 11 to 20 visitors require two Customer’s Authorized Personnel, 21 to 30 visitors require three Customer’s Authorized Personnel, etc. Data Centre tours require the prior approval of Data Centre Management. Tour approval must be scheduled at least three (3) business days in advance of the tour date. To expedite tour Visitor processing, Security Operations must be provided a list of such tour Visitors’ names at least one (1) business day prior to the tour date.

Customer’s Authorized Personnel are responsible for understanding the locations where escorted access is allowed and for ensuring that escorted TOUR Visitors are not permitted to enter any other area in the facility. The Customer and the Customer’s Authorized Personnel are responsible for the actions and safety of the tour Visitors while they are attending at the Qu Data Centre. Please contact your Account Representative to schedule Data Centre tours.

Visitor Access

All temporary Customer guest Visitors will be issued a temporary visitor ID Badge and must be escorted at all times by the Customer’s Authorized Personnel.

To eliminate the potential for unauthorized access or tailgating, Customer’s Authorized Personnel are only allowed to escort up to five (5) Visitors at a time. Tour groups of six (6) or more Visitors are subject to Data Centre Tour Rules.

Temporary or Lost / Defective ID Badges

Any ID Badge holder who has forgotten or lost their ID Badge must report to Security Operations Center.

Data Centre Cage and Cabinet Security Policy

All cages and cabinets within the Customer Area come standard with a lock. In Data Centers where cabinets have key locks, Qu gives Customers the option of being issued a key on a permanent basis or to sign out a key from the Security Operations Center as necessary. For an additional fee, Qu will install, manage, and maintain proximity and/or biometric readers to such cages and cabinets in replacement of locks and keys. Customers are not allowed to install their own security surveillance systems, except for video surveillance cameras that are pre-approved by Qu in writing. The Customer is not permitted to alter, change, or install any locking mechanism on or to the racks and changes within the Customer Area. Additionally, the Customer is not permitted to alter or change any Qu owned cabinet or rack. This includes but is not limited to removal of doors, drilling or mounting equipment to the exterior of the cabinet or rack.

Access Control

Only Qu approved and authorized security measures will be installed in by the Customer on or to the Customer Area. If the Customer wants to install proximity readers, biometric readers, or other custom control measures in or on your space this must be approved in writing by Qu Security. Customers must engage Qu Account Representative for a Scope of Work to be furnished by the Security Operations Center, which shall be at additional cost to the Customer.

WAP in Customer Space

The Customer may not install Wireless Access Point (WAP) in the Data Centre facility.

Hot and Cold Aisle Compliance

All Customers must receive approval from Qu with regard to hot and cold aisle layout configuration and adhere to those requirements prior to equipment installation.

Special venting configurations must be pre-approved and will incur additional set-up costs.

Any void in rack space must be closed with a blanking panel. Periodic compliance audits will be conducted; and when violations are discovered, the Customer will be notified and will be required to remedy such violation within three (3) business days.

Video Surveillance Policy

Upon written approval from Qu, the customer may install video surveillance equipment with the following provisions.

- Customer must supply their own cameras, mounting kits and installation services,
- Customer owned surveillance systems will not be interconnected with Qu surveillance systems,
- No camera installations may occur without the successful completion of the Contractor Work Rules test,
- All Customer contractors must adhere to Qu' Data Centre Work Rules: SV1-FAC Policy. This policy requires Contractors to review Qu policy materials. Customer must reasonably cause its contractors to read and understand this policy.

- All surveillance cameras are to be installed: Securely installed to assure that they do not present a safety issue. (falling, head injuries, etc.).
- Customer (or any of its representative) may not lift the tiled Data Centre floor, or enter into the plenum above the cage.
- May not block any Qu surveillance equipment.
- May not interfere with cage or cabinet access.
- Must have a fixed camera view feature limited so the maximum field of view includes only the customer's cabinets in the cage in which the cabinets are located. No cameras that are pan, tilt, or zoom enabled will be installed.
- May not include audio recording.
- May not view other customer's cages or other parts of the Data Center.

After installation, the Customer must demonstrate to Qu Data Centre Facilities Management and Security that their installation meets the above requirements. Qu will perform periodic unannounced checks and may request verification that requirements have been satisfied.

Qu will not respond to Customer owned video surveillance equipment alarms; however, the Customer request Qu to do so, such response will be billed to the Customer at Qu's then current remote hands service rates.

Photography Policy

Unless otherwise pre-approved by the Data Centre manager, Customers are prohibited from taking photographs (analog, digital, still, video, camera phone, or web cam) inside any Data Center; any photography permission given to a Customer may be subject to a written agreement between Qu and the Customer. Any Visitor engaged in unauthorized photography at a Data Centre will be reported to Security Operations immediately for intervention and all photographic records will be required to be destroyed or deleted.

Building Evacuation Policy

If the Data Centre fire alarm or other life safety alarm is activated, all Visitors must immediately evacuate the Data Centre and report to an assembly point free and clear of danger. Evacuees are to remain at the assembly point until they are informed that they may leave the premises or enter the Data Centre by Security Operations, Data Centre Management, or the local authorities.

Parking Lot Policy

Customer designated parking spaces are restricted for Customer use only. Handicapped parking spaces are restricted to those vehicles displaying a current handicapped license plate or hanging placard issued by the respective provincial government authority; these spaces are designated with the International Symbol of Access (wheelchair symbol) or a blue curb.

Floor Tile Lifting Policy and Under Raised Floor Access

Customers are prohibited from lifting Data Centre floor tiles. Only Qu employees may access and work below the raised floor area. If access is necessary during installation, please contact the onsite Qu Data Centre personnel or Service Desk in order to request such access. There may be an additional fee for accessing the space underneath the floor tiles.

Crash Carts and Tools

Crash carts (mobile units housing a keyboard, monitor and mouse) and tools are provided on a limited basis as a courtesy to Customers. They are provided on a first-come, first-served basis. Crash carts are required to be signed out with the onsite Qu Data Centre personnel and returned within a 24-hour window. As crash carts may not always be available, and therefore it is encouraged that workers to come prepared to conduct their intended work.

Data Centre Safety and Environmental Policy

- Customers must keep their Customer Areas, including cages clean and free of debris at all times. Empty cardboard boxes and container must be immediately removed by the Customer from the Customer Area. Due to fire and safety requirements, this policy is strictly enforced and Qu reserves the right to remove any cardboard, paper, debris etc. from any and all Customer Area (such as cages and racks) in which case a minimum of one (1) hour remote hands Fee will be charged to the offending Customer.
- Customers may not store materials or paper products (**including cardboard and boxes**) anywhere in the Data Center. Unused cabling and equipment must be properly stored. Cabling may not be draped in aisle ways or hinder clearance around cabinets.
- Customers must keep tile vents clear of any obstruction. Non-functioning equipment and miscellaneous items must be stored inside your cage area only and only on a temporary basis.

Prohibited Materials in Qu Data Centers

The following items are prohibited in Qu Data Centres:

- Food or drink – prohibited on the raised floor
- Tobacco products (including smokeless) – prohibited on the raised floor
- Explosives, firearms or weapons of any type
- Hazardous materials or other chemicals
- Alcohol, illegal drugs, as well as other intoxicants
- Magnets and electromagnetic devices
- Radioactive materials
- Photography equipment (unless preauthorized by Data Centre Management) or recording equipment of any kind (other than tape backup equipment)
- UPS equipment, other than what is provided by Qu, is strictly prohibited.



- Paper products (other than equipment manuals) or other combustible materials of any kind, including cardboard and boxes

Bolt-down, Seismic Bracing & Grounding of Cabinets and Racks

Structural bracing systems must meet or exceed seismic design requirements of local building codes for lateral seismic design. Customers are responsible for all costs associated with seismic bracing of cabinets and racks.

All cabinets and racks in all Data Centers must be anchored, braced and grounded in accordance with the requirements of the 2005 International Building Code and the National Electric Code. All Customer-owned cabinets will be installed only by Qu personnel.

Customer Cabling

Cabling within customer cages must be installed in an appropriate industry standard discipline and professional manner. Cabling must be properly run and secured within cabinets, by using overhead and vertical cable management devices. Cabling must be installed in a safe manner so that it in no way impedes aisles, floor ways or entranceways. Qu standard cable management is accomplished by overhead wiring trays. All other wire management equipment will incur an additional fee. All cabling must be plenum rated and meet the UL minimum code standards. Qu recommends clear labeling at each end of all installed cables. Qu reserves the right to remove any non-compliant cabling after notification of a cabling violation. Qu Professional Services are available to Project Manage cabling installation and cabling clean up. Please contact your Qu Account Team for further information.

This policy is referenced in Qu's Master Services Agreement