CSQUARE

Customer Services Guide

Version: 1.1.1
July 23, 2026

© 2026, Phoenix Infrastructure LLC, a Delaware limited liability company and its affiliates dba Csquare. All rights reserved. All other marks and names mentioned herein may be trademarks of Csquare or another company. The products and services described herein may be intellectual property of Csquare or of another company and protected by one or more U.S. or international copyright or intellectual property laws. The terms set forth in this Csquare Customer Services Guide ("Customer Services Guide") apply to services provided by Csquare to customers from time to time (the "Services"). This Customer Services Guide constitutes proprietary, confidential information of Csquare, and may not be disclosed or used except as may be provided in the terms and conditions of the Master Services Agreement pursuant to which customer has been authorized to use the Services and this Customer Services Guide.

1 Welcome 3
1.1 Customer Account Identification 3
1.2 Data Center Locations 4
2 Support 6
2.1 Assistance via Phone or Email 6
2.2 Csquare Customer Portal 6
2.3 Support Priority Definitions 9
2.4 Event and Maintenance Notifications 10
2.5 Support Response and Escalation 10
2.6 Customer Success Services 10
3 Data Center Security and Physical Access 12
3.1 Authorizing Physical Access 12
3.2 Access Badges 13
3.3 Data Center Common Areas 16
4 Colocation Services 18
4.1 Secure Cabinet 18
4.2 Secure Cages 18
4.3 Power 21
4.4 Remote Hands 22
4.5 Customer Packages and Shipments 24
5 Interconnection and Network Services 27
5.1 Interconnection Offerings 27
5.2 On Demand Services 31
6 Policies 35
6.1 Compliance, Reports and Audits 35
6.2 Data Center Policies 36
6.3 Colocation Environment Policies 38
6.4 Data Center Power Policy 42
6.5 Connectivity Policies 44
6.6 Month-to-Month Services 48
7 Business Continuity 48
7.1 Infrastructure Maintenance 49

1 Welcome

At Csquare, our data center services enable flexibility that allows our customers to accelerate innovation. We are happy to have you as part of our ecosystem and look forward to supporting you as your business evolves.

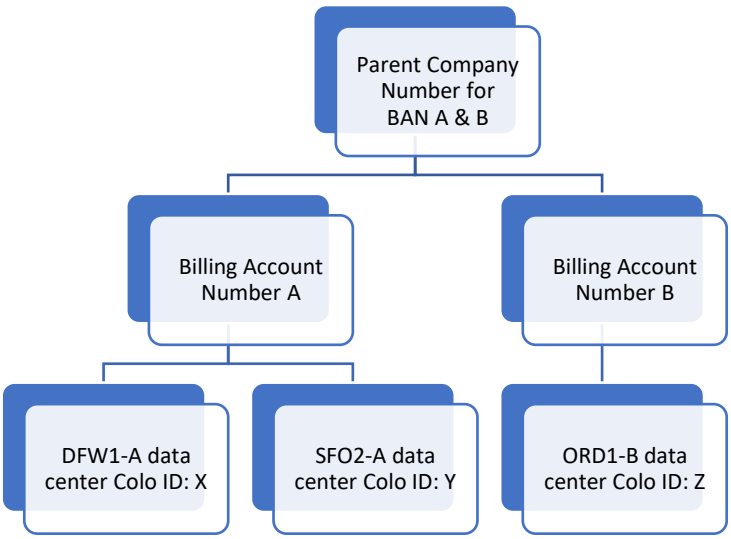
The Customer Services Guide defines how to obtain support, our data center policies and product offerings. Csquare recommends bookmarking this guide for reference. Our customers, including their visitors, contractors and/or vendors that may access the services, must adhere to the policies set out in this guide. Csquare reserves the right to update this document from time to time.

The latest version of this Customer Services Guide can be found at: https://csquare.com/customer-guides

1.1 Customer Account Identification

Csquare customers are assigned unique identifiers for their account and provided this information as part of their onboarding experience. Below are the definitions used for customer account identification:

- **Company Number:** also known as Billing Parent ID or Parent Account is the top-level account that all customer colocation environments are associated with.
- **Billing Account Number (BAN):** is used for identifying the customer invoicing entity.
- **Colo ID (Account Group):** Colo ID, also referred to as Account Group, is a unique number assigned to a specific colocation environment and corresponding services within a specific data center pod. Pods are defined as data center white space (colocation area) powered by their own separate redundant power and indicated by a letter suffix after the data center code. Support tickets and management in the Csquare Customer Portal is at the Colo ID level.



1.2 Data Center Locations

Below is the list of Csquare data centers. Csquare data center code names are based off the nearest international airport with a suffix letter representing pods within the data centers.

MARKET	CODE/POD	STREET ADDRESS
ALBUQUERQUE	ABQ1-A ABQ1-B	400 Tijeras Avenue Northwest, Albuquerque, NM 87102
ATLANTA	ATL1-A ATL1-B ATL1-C	375 Riverside Parkway #150, Lithia Springs, GA 30122
	ATL1-D	375 Riverside Parkway #100, Lithia Springs, GA 30122
NASHVILLE	BNA1-A	1398 Gateway Drive, Gallatin, TN 37066
BOSTON	BOS1-A	580 Winter St, Waltham, MA 02451
	BOS1-B	112 2nd Ave, Waltham, MA 02451
	BOS4-A	486 Arsenal Way, Watertown, MA 02472
COLUMBUS	CMH1-A	8180 Green Meadows Dr, Lewis Center, OH 43035
DALLAS	DFW1-A DFW1-B DFW1-C DFW1-D	14901 FAA Blvd, Fort Worth, TX 76155
	DFW2-A	900 Guardians Way, Allen, TX 75013
	DFW3-A	11830 Webb Chapel Rd. Suite 200, Dallas, TX 75234
DENVER	DEN1-A DEN1-B	9110-9180 Commerce Center Cir, Littleton, CO 80129
	DEN2-A	8534 Concord Center Dr, Englewood, CO 80112
NEW JERSEY	EWR2-A EWR2-B EWR2-E EWR2-F	300 JFK Boulevard East, 1/2/3rd Floor, Weehawken, NJ 07086
	EWR2-C EWR2-D	1919 Park Ave, Weehawken, NJ 07086
	EWR3-A EWR3-C	3 Corporate Place, Piscataway, NJ 08854
	EWR5-A	15 Enterprise Ave North, Secaucus, NJ 07094
WASHINGTON DC	IAD1-C IAD1-E	21110 Ridgetop Cir, Sterling, VA 20166
	IAD1-B	45845 Nokes Blvd, Sterling, VA 20166
	IAD1-A IAD1-F	45901 Nokes Blvd, Sterling, VA 20166
	IAD2-A IAD2-B	22810-22860 International Dr, Sterling, VA 20166
	IAD3-A	22995 Wilder Ct, Dulles, VA 20166
	IAD4-A	21571 Beaumeade Circle, Ashburn, VA 20147
	IAD4-B	21561 Beaumeade Circle, Ashburn, VA 20147
LOS ANGELES	LAX3-A LAX3-B	17836 Gillette Avenue, Irvine, CA 92614
	LAX4-A	2301 West 120th Street, Hawthorne, CA 90250
	LAX5-A	2681 Kelvin Ave, Irvine, CA 92614

LONDON	LHR2-A	7 Greenwich View Place, London, E14 9NN, United Kingdom
	LHR2-B	6 Greenwich View Place, London, E14 9NN, United Kingdom
	LHR3-A	Eskdale Rd, Winnersh, Triangle, Wokingham RG41 5TS, United Kingdom
MINNEAPOLIS	MSP1-A MSP1-B	4450 Dean Lakes Boulevard, Shakopee, MN 55379
CHICAGO	ORD1-A	350 E Cermak Rd, Chicago, IL 60616 (7th Fl)
	ORD1-B ORD1-C ORD1-D	350 E Cermak Rd, Chicago, IL 60616 (4th/8th Fl)
	ORD2-A	2425 Busse Rd, Elk Grove Village, IL 60007
	ORD4-A	4513 Western Ave, Lisle, IL 60532
PHOENIX	PHX1-A PHX1-B PHX1-C PHX1-D	615 North 48th Street, Phoenix, AZ 85008
	PHX3-A	1301 W University Drive, Mesa, AZ 85201
SEATTLE	SEA1-A	12301 Tukwila International Blvd, Tukwila, WA 98168
	SEA1-B	3355 S 120th Pl, Tukwila, WA 98168
	SEA2-A	6101 S 180th St, Tukwila, WA 98188
	SEA3-A	17300 Hwy 99, Lynnwood, WA 98037
SAN FRANCISCO	SFO1-B	2403 Walsh Ave, Santa Clara, CA 95051
	SFO1-A SFO1-C	2401 Walsh Ave, Santa Clara, CA 95051
	SFO2-A	4700 Old Ironsides Dr, Santa Clara, CA 95054
	SFO2-B	4650 Old Ironsides Dr, Santa Clara, CA 95054
	SFO3-A	1400 Kifer Rd, Sunnyvale, CA 94086
	SFO4-A	1550 Space Park Dr, Santa Clara, CA 95054
	SFO4-B	1500 Space Park Dr, Santa Clara, CA 95054
	SFO9-A	3175 Spring St, Redwood City, CA 94063
TAMPA	TPA1-A	9310 Florida Palm Dr, Tampa, FL 33619
TORONTO	YYZ1-A	6800 Millcreek Dr, Mississauga, ON L5N 4J9, Canada
	YYZ2-A	4175 14th Ave, Markham, ON L3R 5R5, Canada

In addition to Csquare's data centers, Csquare also has a presence in several other key data center locations in which it offers colocation services. Please contact your account team for more information on these locations.

2 Support

Csquare provides phone, email and online portal support 24x7x365, with the ability for customers to self-manage many elements of support through the Customer Portal.

2.1 Assistance via Phone or Email

Csquare provides 24x7x365 phone support for customers to receive support for critical issues.

When calling Csquare Customer Care, callers will need to provide their full name, email address and Colo ID number to the Csquare support representative. For security purposes:

- The Csquare representative will email a code to the caller's registered email address which must be provided to authorize support tickets.
- Data center access authorization and portal contact changes can only be made through the Customer Portal.
- Only email addresses that are registered in the Customer Portal will be processed for security purposes. Unregistered email addresses will receive a response directing the individual on how to obtain support.

Customer Care Phone Numbers:

- **US: 1-855-699-8372**
- **International: +1-469-270-6755**

Customer Care Email:

- **CustomerCare@Csquare.com**

IMPORTANT:

For critical service-impacting issues, please open an outage case in the Customer Portal with all the required information to address the issue, then contact Csquare via phone to elevate the priority status for timely resolution.

2.2 Csquare Customer Portal

The Csquare Customer Portal or "Customer Portal" provides an easy-to-use solution for monitoring, reporting, and obtaining support for your Csquare colocation and networking services.

- Create, manage, and monitor support tickets and orders
- View of portal contacts with different privileges
- Authorize physical access to a colocation environment
- Request Remote Hands assistance
- Manage and track shipments
- Manage and monitor Csquare network services
- View inventory of cross connects, cages, cabinets, and power circuits
- Download compliance reports
- Receive data center maintenance and other important notifications

Csquare Customer Portal: https://portal.Csquare.com

For detailed instructions on how to use the portal, visit https://docs.csquare.com

2.2.1 Portal Contacts

Portal contacts are users registered in the Customer Portal. Customer must maintain this list of users and ensure there is at least one contact designated as a “Portal Admin” user. Csquare is not responsible for missed notifications if contacts have left the customer's company.

For new accounts, the technical contact from the service order will be assigned as the initial Portal Admin role. The Portal Admin will be invited to register and then be able to invite other users.

- Portal login information should not be shared across multiple users. Each user should have a unique portal login.
- More than one user can be a Portal Admin for a Colo ID.
- All Colo IDs should have a Portal Admin (recommended minimum of 2).
- Contacts can only see the information for the Colo IDs to which they are assigned.

When adding new contacts, ensure the first name and last name of the invited user matches the name on any government ID for that user to access a data center.

Customers are responsible for the actions of the users and third parties it invites to the Csquare portal and the protection of any Csquare confidential information available on the portal.

The following table describes the contacts and portal roles that can be assigned.

PORTAL CONTACT TYPE	RESPONSIBILITIES
PORTAL ADMIN	• Management of the portal for the Colo IDs to which they are assigned • Able to perform all portal functions, including creating and updating contacts, ordering services and granting physical access to data centers
PORTAL USER	• View and create tickets • Users can be granted elevated user permission(s) by a Portal Admin.
NON-PORTAL USER	• No portal login • Can be added to case watchlists, to be notified on case updates

Portal Admins will automatically be assigned the following attributes and Portal Users can be given specific attributes by a Portal Admin.

CONTACT ATTRIBUTE	RESPONSIBILITIES
DIGITAL EXCHANGE MANAGER	• Configure and receive alerts on Csquare Digital Exchange services
TEMP ACCESS MANAGER	• Grant/revoke temporary data center access
PERMANENT ACCESS MANAGER	• Grant/revoke permanent data center access
ORDER CREATOR	• Create and view orders
BILLING VIEWER	• View invoices
MARKETPLACE MANAGER	• Ability to manage the customer’s storefront within the Csquare Marketplace (if applicable)

The following attribute can be set on a specific contact:

CONTACT ATTRIBUTE	RESPONSIBILITIES
METAL KEY MANAGER	• The individual who has been permanently issued the customer's key to a specific cage or a cabinet for the Colo ID

Contacts can select what email notifications they wish to receive by assigning one or more of the below attributes:

CONTACT ATTRIBUTE	RESPONSIBILITIES
ALL CASES & ORDERS	• Receive emailed notifications on case/order creation and updates for the Colo IDs which they are assigned
DATA CENTER MAINTENANCE AND EVENTS	• Receive emailed maintenance notifications, data center events and related updates for data centers associated to their Colo IDs
PHYSICAL ACCESS	• Receive email notifications when multi factor authentication is modified on their Colo IDs
PORTAL ACCESS	• Receive email notifications when contacts log into the Customer Portal
SHIPPING NOTIFICATION	• Receive email notification on unexpected shipments or deliveries for the Colo IDs which they are assigned

Contacts are required to reset their passwords every six months. Contacts that do not reset their passwords or accept a portal invite within two months of the request will be automatically deactivated and must be reactivated by a Portal Admin.

Changes to existing contacts or the addition of new contacts can only be made by Portal Admins through the Customer Portal.

2.3 Support Priority Definitions

The following table describes the priority definitions for support tickets.

PRIORITY	DESCRIPTION
P1 **CRITICAL**	**Core business interrupted; operations severely impacted or pending imminent failure.** • A customer critical system or component is down • Imminent outage of critical business system if not resolved • SLA defined critical process is not functioning • All network traffic has stopped • Circuit power both primary and secondary failure • If a customer representative is no longer available to assist, priority may be reduced.
P2 **HIGH**	**Core business functioning at reduced capability, or loss of redundancy for critical systems.** • A critical system or component is experiencing degradation of service • A critical business system has lost redundancy • Customer is experiencing degradation of service • SLA defined critical process is no longer resilient • Failure of primary on a network redundant pair • Circuit power primary failure but secondary active
P3 **MEDIUM**	**Issue with non-business critical systems.** • Non-business critical system issue but no degradation of the Customer's ability to conduct business • A non-critical business system has lost redundancy • An incident indicative of non-SLA or non-contractual issues
P4 **LOW**	**Investigative action or request for information.** • Limited impact issue that does not require immediate attention (not outage related) • Notification of incoming shipments and requests for physical access • Low level request required to investigate minor issues • Requests information or a report • Other non-impacting service requests

Csquare reserves the right to adjust the priority of customer submitted tickets based on these definitions.

2.4 Event and Maintenance Notifications

Notifications are sent from noreply@Csquare.com email address, which is not monitored and will return an automated response. Customers should ensure this email is whitelisted in their spam filters. Users needing to respond to a notification should respond in the Customer Portal or call Customer Care.

Customer Specific Events

Events that only impact a specific customer, such as localized temperature/humidity alerts, power issues within the data center etc. are posted to the portal and sent via email to all registered portal users for the affected Colo ID who have opted in to maintenance and event notifications.

Data Center-Wide Events

Routine scheduled maintenance impacting redundancy, utility to generator testing, as well as outages affecting multiple customers will trigger data center wide notifications sent to all registered portal users for the affected Colo ID who have opted in to maintenance and event notifications. **See Section 7.1 Infrastructure Maintenance.** These notifications as well as non-impacting customer maintenance will be posted to the Customer Portal.

Csquare strives to keep customers informed of changes and maintenance. Additional information about the impact of a particular event or maintenance on a customer's environment can be requested by contacting Customer Care or opening up a ticket in the Customer Portal.

2.5 Support Response and Escalation

Tickets are assigned priority based on **Section 2.3 Support Priority Definitions.** For Csquare generated events or customer generated tickets, our initial response objectives are as follows:

Ticket/Event priority	Initial response objective
Priority 1	≤30 minutes
Priority 2	2-4 Hours
Priority 3	Within 1 business day
Priority 4	Within 1 business day

To escalate an existing ticket of any priority, please contact Customer Care. Customer Care will escalate with the appropriate operations team and, if necessary, management.

2.6 Customer Success Services

We have three Customer Success service tiers. All customers are assigned an Essential Customer Success Manager (CSM). A CSM will reach out to a new customer to help assist in onboarding and the introduction of Csquare's services. CSM's do not provide implementation services or deployment project management, but facilitate escalation of customer issues, if any arise. Post installation, the CSM is responsible for the customer relationship, including assisting with questions related to billing, contract renewals, and service issues.

The Customer Success Advanced tier offers proactive services that include monthly business reviews with detailed standardized reporting. Customers also can use their CSM as support for invoice management. The Advanced tier covers services for a single data center. Customers with multiple data centers must purchase an additional package for each data center they wish to include or consider purchasing the Enterprise service tier.

The Customer Success Enterprise tier expands reporting to all the customers' colocation environments in multiple data centers and allows custom reporting. Additionally, Enterprise authorizes the CSM to access the customer's Csquare Portal dashboard to manage portal contacts, set up access authorizations to data centers, create cases and manage shipments on the customer's behalf, as needed.

	Essential *Included for all customers*	**Advanced** *Monthly fee per data center*	**Enterprise** *Monthly fee per customer*
Initial Account Set-up	✓	✓	✓
Sales Support and Contract Renewals	✓	✓	✓
Customer Escalations (Billing)	✓	✓	✓
Customer Satisfaction Management	✓	✓	✓
Enhanced Support and Portal Assistance		✓	✓
Monthly Business Review		✓	✓
Power utilization report per rack		✓	✓
Case status reporting by type		✓	✓
Remote Hands utilization		✓	✓
Temperature & humidity reporting		✓	✓
Portal contact review		✓	✓
Network utilization of Csquare products		✓	✓
Access log review		✓	✓
Shipping/package reporting		✓	✓
Maintenance schedules		✓	✓
Incident reviews		✓	✓
Support for Invoice Management		✓	✓
Administration on Customer's Behalf			✓
Case creation/administration			✓
Portal contact creation/administration			✓
Site access creation/administration			✓
Shipping creation/administration			✓

Note: Custom and/or ad-hoc reports can be purchased via a Remote Hands case on the Csquare Portal (2 hours Remote Hands minimum per report).

3 Data Center Security and Physical Access

Csquare enforces physical security practices that include physical monitoring, intrusion detection systems, locks and access barriers, and screening physical access to data center facilities and equipment.

- All individuals entering a Csquare data center are required to adhere to the policies defined in this document.
- The customer is responsible and assumes liability for the actions of all individuals it authorizes (including vendors) to enter Csquare facilities on the customer's behalf.
- Csquare will refuse access to the data center and customer environments to anyone without valid access authorization. Third parties must have permanent or temporary access granted by the customer.

The Csquare physical security organization provides global physical security operations, security systems, access administration, and security controls within the Csquare data centers.

- Security includes data centers staffed 24x7, biometrics / pass card access, monitored and alarmed doors, and mandatory access to the data center floor via a mantrap.
- Each data center has a Security Operations Center (SOC) or a security desk. Security personnel control access to the data center, monitor security alarms and Closed-Circuit Television (CCTV) cameras, and manage all security-related issues from the SOC or security desk.
- The Csquare Physical Security Command Center (PSCC) provides global, 24x7 support to the local data center security teams with remote monitoring, management, administration, and maintenance of the access control systems and CCTV video surveillance systems. The PSCC may direct local data center security in response to critical alarms, physical security incidents and critical events involving law enforcement, fire, or emergency medical personnel.
- Data centers utilize 24x7 CCTV to monitor key internal and external areas including lobbies, common areas, customer lounge, data center floor space, admin areas, and engineering plant areas. Customer environments are not included within Csquare CCTV surveillance. Video recordings are retained for at least 90 days for exterior and internal critical areas and 30 days for non-critical areas such as common areas.

3.1 Authorizing Physical Access

Csquare's data center staff use customer contact lists submitted from the Customer Portal to verify access authorizations prior to granting physical access to the data center. Data center access authorization may be granted on a permanent or temporary basis.

- When providing visitor information, **the first and last name of the visitor must match their name as it appears on their unexpired government-issued photo identification.**
- Customers are responsible for maintaining their physical access authorizations. Csquare is not responsible for allowing access to individuals such as ex-employees who are still authorized for physical access to a data center.
- Customers are responsible for the actions of any individual they authorize while they are within the facility and surrounding areas.

Data center access authorizations must be made through the Customer Portal. Any requests submitted via phone or email will be redirected to the Customer Portal to ensure requests are authorized via username/password and multi-factor authentication if enabled.

	PERMANENT ACCESS	TEMPORARY ACCESS
DEFINITION	Access to a data center at any time for specific cages or cabinets	One-time scheduled access for a limited time for specific cage or cabinets
USE CASE	Employees and vendors that visit the data center regularly	A vendor or employee visiting the data center to conduct a specific task at a defined time
DURATION	Until the authorization is revoked	Start time/date and end time/date as specified in the authorization
AUTHORIZED BY	"Portal Admin," or "Portal User" with "Permanent Access Manager" set	"Portal Admin," or "Portal User" with "Temp Access Manager" set
UNSUPERVISED ACCESS	Access to the data center raised floor and customer specified cage/cabinet	Access to the data center raised floor and customer specified cage/cabinet
CUSTOMER SUPERVISED **(TEMP ACCESS)**	n/a	The visitor(s) will not be allowed to enter the facility unescorted, and a customer representative with a permanent badge must remain with the visitor(s) while they are within the data center
CSQUARE ESCORTED **(TEMP ACCESS)**	n/a	The visitor(s) will not be allowed to enter the facility unescorted and data center staff will remain with the visitor(s) while they are within the data center **Note: Escorted access is a billable service via Remote Hands**

Visitor activity reports on who entered a data center can be viewed and downloaded from the Customer Portal.

3.2 Access Badges

Access badges are utilized within the data center to allow access to the facility and a specific customer's colocation environment. To control access to the data center and prevent tailgating, Csquare utilizes mantraps combined with a two-factor authentication for access beyond the front lobby. Data center staff cannot issue access badges to visitors who do not have a valid access authorization. Visitors who arrive at the facility without authorization must contact a "Portal Admin" for their account to authorize access.

All visitors must submit to a search of any bags or packages when requested at the security desk before entering the data center. Csquare may require additional screening before entering the facility, depending on local security policies and health screening requirements.

Biometric scanners: Csquare may utilize biometric scanners to authenticate visitors when accessing the data center, and visitors may be required to sign a biometric disclosure form prior to entering the data center. Visitors not willing to sign a biometric disclosure form can only be granted temporary escorted access that will be billed at Remote Hands rates for the duration of the visit.

Biometric disclosure: All visitors who have not already acknowledged a biometric disclosure form for that jurisdiction of the data center they are visiting will be required to accept a disclosure before visiting a data center. Acknowledgement of a Biometric form covers all data centers in that jurisdiction.

The relevant biometric disclosure forms can be found at:

US (excluding California) - https://csquare.com/docs/biometric_US

US (California) - https://csquare.com/docs/biometric_California

Canada - https://csquare.com/docs/biometric_Canada

Two-factor authentication is always required to enter the secured, raised floor colocation areas of the data center, and involves granting a person access based upon a combination of:

- Presenting a valid Csquare access badge
- Verification of the badge holder using either:
    - Finger or hand scan
    - Personal identification number (PIN) code
    - Validation of valid Government ID by Csquare data center security

Individuals granted permanent access will have unescorted access to the customer's environment. Temporary access is unescorted unless escorted access by the customer or Csquare staff, is specified in the access authorization request.

3.2.1 Kiosk locations

Data centers with a sign-in kiosk in the lobby area require visitors to enter their name into the kiosk prior to collecting their badge. For both permanent access and temporary access, badges must be collected from the security desk when entering the facility and then returned when leaving the facility.

3.2.2 Issuing Access Badges

All temporary visitors are required to pick up access badges from the security desk prior to entry to the facility.

- Temporary or visitor access badges are valid only for the duration specified in the access authorization.
- All individuals assigned temporary badges must return the badges to data center security or deposit them in the key and badge drop box (where available) when leaving the data center.

Permanent access visitors will be required to have their biometric data captured on their first visit to a data center.

- Some data centers (non-kiosk data centers) allow permanent visitors to retain their badges and use the same badge for other non-kiosk data centers they are authorized to enter.
- Badge issuing hours are 8:00 a.m. to 5:00 p.m. local time, Monday through Friday. If a permanent badge cannot be issued immediately, a temporary badge will be provided while the permanent badge is being set up.
- Permanent access visitors for kiosk enabled data centers will be required to pick up and return their badges for every visit.

All visitors must show a current and valid government issued photo ID prior to being issued a badge. Expired ID, company badges or any other forms of identification not issued by government agencies, such as credit cards, are not acceptable. Eligible IDs are limited to the following:

- Driver's license or State Issued ID
- Government-issued identification card
- Passport
- Military identification card

Csquare badges are property of Csquare, are revocable, not transferable, and may not be shared with other individuals for any reason. They may not be tampered with and must be returned by the individual upon request. Visitors must wear access badges at, or above the waist, and must ensure they are always visible.

Permanent customer badges remain active until the badge holder's authorization is revoked by the customer. Badges retained by visitors, that are unused for more than 90 consecutive days will be disabled without prior notice to the badge holder. A badge holder may request re-enablement of their badge on their next visit to the data center. Any visitor retained badges which remain unused for twelve consecutive months will be deactivated. Upon deactivation, all biometric information will be deleted. Csquare will permanently destroy all cardholder records in the access control system two years after (a) the associated badge is rendered inactive, or (b) the last recorded badge activity, whichever occurs first.

3.2.3 Access to Customer Cage / Cabinet

Access to a customer's specific cabinet or cage within the data center varies by facility and customer selected access options. Csquare access badges and biometric access can be controlled and managed centrally, while key or combination lock access is customer managed.

Csquare may enter the customer area and/or access customer materials/equipment for the purpose of installation, inspection, removal, relocation, replacement, or maintenance of the Csquare services in an emergency or as otherwise necessary for Csquare to provide the services.

Metal Key Management (where applicable)

Csquare keeps a minimum of two keys for each customer cage or vault area, one loaner to be issued to customer and one back-up that is always retained by Csquare. Csquare secures all metal keys within the Security Operations Center.

- Visitors authorized by customers for permanent or temporary data center access may obtain the loaner key from Csquare. The person assigned the loaner key is responsible for returning the key to data center security or to the key and badge drop box, when leaving the data center. Any loaner key that is reported as having left the data center premises is considered lost and may result in Csquare securing the customer colocation space with a chain and lock, in which case access to the customer environment will be via escort only. In such instances, Csquare may re-key the customer's environment at the customer's expense.
- Customers may appoint a "Metal Key Manager" in the Customer Portal. It is the sole responsibility of the customer's Metal Key Manager, and not Csquare, to manage ownership, distribution, possession, and use of the key. Metal Key Managers may make as many copies of the key as needed. By agreeing to manage the key, customers acknowledge and accept that any person with a valid Csquare permanent access badge and key has unrestricted access to the customer's colocation space, and Csquare is not responsible for any unauthorized access to the customer's space.

Combination codes (where applicable)

Customers are responsible for maintaining their combination code(s) as well as providing the appropriate combination code to their authorized contacts to access the customer's environment. If the combination code is lost/forgotten, or if the customer does not wish to provide the combination code to an authorized contact to access the customer environment, the customer must submit a Remote Hands ticket via the Customer Portal to request a Csquare escort for assistance, and Remote Hands charges will apply.

3.2.4 Exiting the Data Center

All individuals must exit the data center through the lobby area mantrap.

At data centers equipped with a check-in kiosk, all badges and keys must be returned to security before leaving the data center. At non-kiosk data centers, all temporary badges must be returned. Visitors may also be required to sign out at the guard desk. Visitors should check with security on the specific exit procedure for the data center.

3.2.5 Data Center Tours

Both existing customers and prospective customers can request a tour of a Csquare data center.

Customers should schedule tours with as much lead time as possible as tours require the approval of data center management. Customers must obtain tour approval from Csquare data center management at least three business days before the tour date.

To expedite visitor processing, the tour request should include each attendee's first name and last name as it appears on their government-issued photo identification.

- Changes to the list of attendees should be finalized at least one business day before the tour.
- The requestor of the tour is responsible for the actions and safety of the visitors while in Csquare's data center.

Prospective customers can request a data center tour by contacting their Csquare account representative.

Tours are permitted for a customer's auditor(s) to assess a facility or for operational reviews. These tours must be requested by the Customer on behalf of the auditor. If a data center walkthrough is booked for the purpose of an audit, the duration of the tour will be billed via Remote Hands. **See Section 6.1 Compliance, Reports and Audits.**

3.3 Data Center Common Areas

Data center amenities are available on a first-come, first-served basis for short-term use. Csquare is not responsible for customer information, customer assets or equipment left unattended in common areas. Please review **Section 6 Policies** on use of services in this section.

3.3.1 Parking

Parking is provided for customers during their visit at most of our facilities. Customers must park in designated parking areas only. Csquare is not liable for damage, loss, or theft of vehicles and/or contents while located in a data center parking area.

3.3.2 Work Areas and Lounges

Csquare maintains common work areas and lounges for use by all Csquare customers with colocation space within that data center. Customers that require dedicated office space should work with their Csquare account representative on options and availability. **See Section 4.2.3 Office Space**.

3.3.3 Conference Rooms

Csquare maintains conference rooms for use by customers with colocation space within that data center. Conference rooms are available during normal business hours, at the sole discretion of data center management. Customers must request rooms at least 24 hours in advance via the Customer Portal. Video screens or projectors are available at many locations, but customers should confirm with the data center prior to the meeting if audio and/or visual equipment is required.

Csquare reserves the right to charge for the use of conference rooms, including use for non-data center related activities, scheduling requiring more than two days per week, five days in any given month, or a conference room in a data center the Customer does not have equipment collocated.

3.3.4 Loading Docks

Data centers have loading docks for the shipping and receiving of customer shipments. **See Section 4.5 Customer Packages and Shipments**. Access to loading docks (rollup doors, etc.) is restricted. Customers may be granted access with Csquare personnel supervision during normal business hours. Customers needing after-hours access to loading docks must submit a Remote Hands ticket at least 72 hours' notice to supervise this activity. Remote Hands charges will apply for supervised loading dock access. **See Section 4.4 Remote Hands.**

3.3.5 Staging Areas

Most Csquare data centers have staging areas available to temporarily unpack and configure equipment, prior to installation in customers' cabinets and cages. Equipment assembly, configuration and storage may not be conducted in common work areas or customer lounges.

3.3.6 Common Area Connectivity

Csquare data centers have complimentary Wi-Fi access for visitors within the data center. This service is provided on a best effort basis and Csquare does not guarantee that Wi-Fi will be available throughout the entire data center or 100% availability.

- Csquare guest Wi-Fi credentials can be requested when signing into the facility.
- Csquare guest Wi-Fi is for connectivity or visitors' mobile devices and laptops only.
- The connection is not to be used for connectivity to equipment on the data center floor.

Common area telephones and internet access are for use on a temporary basis for business purposes during the visit only.

4 Colocation Services

Csquare's colocation services range from standalone single cabinets to large cages supporting tens to hundreds of cabinets, all with a wide range of available customizations to support a broad spectrum of business needs.

4.1 Secure Cabinet

Csquare offers a single cabinet, or group of single cabinets, on the data center floor which provides a solution for customers who require small footprint colocation services. Secure Cabinets are sold by the amount of usable power that they are equipped to provide and are delivered in industry standard sizes.

Secure Cabinets are a nominal 45U high 42" deep (40" rack with 2" for doors), with a load rating of 1,250 lbs. maximum. All cabinets have front and rear lockable doors that come standard with either a metal lock with key or combination code, and additional access control options are available.

Customers contract for a Secure Cabinet based on the size of the power circuits selected for the deployment. This power model includes the base infrastructure power charge, and a predefined monthly usage built into a flat monthly rate. Usage of space is included in the monthly charge for the service.

Within the Secure Cabinet, a minimum of one rack unit is reserved for Csquare interconnection panel(s) purchased as Ecosystem Connect. The default position for the Ecosystem Connect patch panel is the top U of the rack, but customers can request alternate positions. **See Section 5.1.1** for more information on Ecosystem Connect.

4.2 Secure Cages

For customers requiring dedicated contiguous space, large numbers of cabinets, or who have specific security and/or access requirements, Csquare offers secure cages in a wide variety of sizes and configurations. Secure cages are sold based on the square footage of the cage space and power contracting model. **See Section 6.4 Data Center Power Policy.**

Secure Cage Build

Cages are built using manufactured panels and are equipped with either one or two sliding doors depending upon the size of the cage and the local fire codes. Standard caging material is either a perforated metal panel or wire mesh, depending on the site. The standard cage wall is 8', and the top of the cage is open.

- Customers requiring higher levels of security may purchase additional options, such as taller panels, cage cap or roof, and/or underfloor skirting as part of their design, as well as visual screening or masking to obscure the contents of the cage.
- The first cage door will be equipped with either a metal key lock or a combination lock. Additional access controls or features are available including, but are not necessarily limited to, Badge-In/Badge-Out, Alarm on Left Open, Biometrics, etc.
- Racks are a nominal 45U high, 24" wide, 42" deep (40" rack with 2" for doors), with a maximum load rating of 2,500 lbs. Racks that will have a loaded weight exceeding 1,250 lbs. may require additional underfloor bracing at customer expense.

Cabinet and Rack Design and Installation Requirements

For the safety of customers and data center staff, all cabinets and racks in all data centers must be anchored and grounded in accordance with the requirements of the applicable building code and the National Electric Code. All customer-provided cabinets and racks must be approved in advance by

Csquare and installed by Csquare personnel. Customers must obtain prior written approval for their cabinet or rack layout from Csquare prior to installation and adhere to those requirements.

Seismic bracing or seismic-rated cabinets are required in facilities that are located in seismically active zones (IBC Seismic Design Categories E&F). Structural bracing systems and customer-provided cabinets and racks must meet or exceed seismic design requirements of local building codes for lateral seismic design. Csquare customers are responsible for all costs associated with seismic bracing of cabinets and racks.

Cage Access Options

Access control options for the colocation product include lock and key, keypad, badge reader, and biometrics (finger/hand scanner). All Csquare-supplied customer cages and cabinets come standard with a metal lock with key or combination code.

Intra-Cage Cabling and Infrastructure

Cabling internal to a customer cage / cabinet, or on the customer's side of an Ecosystem Connect panel is the responsibility of the customer. **See Section 6.3 Colocation Environment Policies**.

Csquare provides external connectivity to a customer's cage through a suite of interconnection, network and on-demand products, which are installed and maintained by Csquare. **See Section 5 Interconnection and Network Services.**

Csquare can perform the design and installation of cabling and infrastructure within a customer's cage or cabinet as part of a service order. Services can include:

- Structured cabling between cabinets
- Vertical cable management
- Panels, jacks, terminations, labeling
- Signal wiring or environmental monitoring
- Closed Circuit TV/DVR systems

4.2.1 Roof Rights

Roof Rights is required for any customer roof-mounted equipment. Roof Rights only authorizes the installation of the equipment on the roof including necessary mounting structures (collectively, "Roof Equipment") by a Csquare-approved installation vendor. Customers are responsible for all installation costs.

- Customers must only use roof space for the equipment specified, and Csquare reserves the right to reject a roof top installation for any reason. Any changes to the Roof Equipment require Csquare's prior written approval and may require a service order or Remote Hands assistance.
- Roof Rights does not include ancillary services such as electricity, telephone services, or internet connectivity. Non-redundant roof top power can be purchased from Csquare separately but is not subject to Csquare's power service level agreement.
- Customers must not use the roof space in any way that interferes with facility operations or any other third-party use of the facility. Customers are responsible for ensuring all customer-provided roof equipment meets all applicable electrical and fire standards.
- All access to the roof space for any activity including repairs or maintenance must be pre-authorized by Csquare. Csquare reserves the right to supervise any access or work conducted on the Roof Equipment as a Remote Hands activity. Csquare does not provide any security monitoring or access control authorization for roof space services and, as such, third parties may have access to the roof space and Roof Equipment.

- Csquare has no liability to the customer for any loss or damage to roof equipment or any interference with the customer's use of the roof space caused by Csquare or a third party.

Roof Rights requires Express Entrance (**See Section 5.1.7**) for connecting a roof-mounted device to the customer's colocation environment. Customers may, at their sole cost and expense, bring telephone facilities and internet connectivity into any such roof space for the operation or use of the roof equipment via Express Entrance.

4.2.2 Storage Lockers and Dedicated Storage Space

Customer storage spaces are available in select data centers.

Storage lockers, where available, can be reserved for a monthly fee and are contracted on a month-to-month basis.

Larger dedicated storage space is offered on a first-come, first-served basis. Customers must contract dedicated storage space for a fixed term. This storage space is billed monthly based on the square footage allocated. Setup charges may be applicable depending on a facilities existing space configurations and customer requirements.

- Customers must not use storage space for any purpose other than storage. Subject to approval by Csquare local site management, customers may be permitted to use storage space for assembly, packaging, unpacking, or other equipment-related activities.
- Customers must comply with all applicable Csquare storage requirements, such as allowing adequate sprinkler head clearance, not blocking any egress pathways, and floor loading. If vertical transportation is used, customers and their authorized representatives must adhere to the load limits of the system. Customers can request assistance in transferring equipment to and from storage from Csquare by submitting a Remote Hands ticket.

4.2.3 Office Space

Office space is available in select data centers and is solely for general office use. The charges for office space are inclusive of janitorial services, HVAC, and facilities maintenance. Standard office electrical outlets are included, but Csquare is not liable to the customer for any electricity failure in such space.

Office space is offered on a first-come, first-served basis and is billed monthly by the square footage allocated. Setup charges may be applicable depending on a facilities' existing space configurations and customer requirements.

Charges do not include, among other matters, telephone services or internet connectivity. Customers shall have the right, at their sole cost and expense, to bring telephone facilities, including PBX, voice mail and other systems, and internet connectivity into their licensed office space. Telecommunication facilities will be subject to charges commensurate with cross-connect and other interconnection services charges.

Kitchen appliances of any size or type are not permitted in office or storage spaces. These include refrigerators, coffee makers, toasters, ovens, crock pots, and warming plates. Fans, portable air conditioners, space heaters, heating pads, heated blankets, or point-of-use UPSs are also prohibited. Use of plug strips, extension cords, or power converters must be inspected and approved by site management prior to introduction to the space. Computing and network equipment and cabling may be used within the space with inspection and approval by site management. These items often require dedicated power or cooling system enhancements, which Csquare reserves the right to charge the customer.

Office spaces are subject to Csquare and local authority safety and compliance inspections. Any findings regarding issues within the customer's control must be remedied by the customer within the time directed in the report.

Customers must not affix or install any items to walls, doors, ceiling, floors, locking systems, or make any changes to lighting, electrical, or other fixtures without site management approval, and follow waste disposal and recycling instructions provided by local site staff. Customers must allow Csquare to perform janitorial services and pest control at regularly scheduled intervals.

4.3 Power

Csquare offers two options for contracting power to a customer colocation space.

- **Allocated power model:** monthly charge for the power allocation based on the number and size of the power circuits deployed within the cage environment. This power model includes the base infrastructure power charge, and a predefined monthly usage built into a flat monthly rate.
- **Metered power model**: a monthly power infrastructure charge based on the number and size of the power circuits deployed within the cage environment, and usage charge based on actual power consumption as measured at the breaker. Usage charges are calculated based on measured consumption, cost of power, and PUE rating, per the following calculation:

  Monthly power usage fee = kWh X rate X PUE

  For purposes of the above equation:

  - kWh = total kW hours used by customer in the calendar month
  - Rate = total cost of power paid by Csquare for powering the data center, divided by total kWh used
  - PUE = total facility power divided by the total IT equipment power

4.3.1 Power Distribution and Circuit Ratings

For North America based locations, Csquare offers standard circuits in 120 volt single-phase and 208 volt, single-phase and three-phase configurations, and in amperage ratings from 20-60. Higher voltage and higher amperage circuits may be available at certain sites via special order. **See Section 6.4 on Data Center Power Policy.**

Phase	Voltage (V)	Amperage (A)	Provisioned Apparent Power (kVA)	Power Factor	Maximum Active Power (kW)	Standard Receptacles
1	120	20	2.40	0.8	1.92	NEMA L5-20R
1	120	30	3.60	0.8	2.88	NEMA L5-30R
1	208	20	4.16	0.8	3.33	NEMA L6-20R
1	208	30	6.24	0.8	4.99	NEMA L6-30R
1	208	50	10.40	0.8	8.32	CS-Series
1	208	60	12.48	0.8	9.98	IEC-60309
3	208	20	7.20	0.8	5.76	NEMA L15-20R (3ØΔ) NEMA L21-20R (3ØY)
3	208	30	10.80	0.8	8.64	NEMA L15-30R (3ØΔ) NEMA L21-30R (3ØY)
3	208	50	17.99	0.8	14.39	CS-Series (Δ)
3	208	60	21.59	0.8	17.27	IEC-60309 (Δ or Y)

For UK locations, Csquare offers circuits in either 230V (Single-Phase) or 400V (Three-Phase), in either 16A or 32A variants, as standard.

Phase	Voltage (V)	Amperage (A)	Provisioned Apparent Power (kVA)	Power Factor	Maximum Active Power (kW)	Standard Receptacles
1	230	16	3.68	0.8	2.94	316C6W 316R6W
1	230	32	7.36	0.8	5.89	332C6W 332R6W
3	400	16	11.07	0.8	8.86	416C6W or 416R6W 516C6W or 516R6W
3	400	32	22.14	0.8	17.72	432C6W or 432R6W 532C6W or 532R6W

4.3.2 Cabinet/Rack Power Distribution Units (PDUs)

Customers may purchase suitable cabinet/rack PDUs (power distribution units) from Csquare or are responsible for providing their own PDUs for use in their cabinet(s) and/or rack(s).

The PDUs can be installed in the cabinet by the customer or by Csquare personnel via a Remote Hands ticket but must be connected to the power receptacle by Csquare personnel under a chargeable Remote Hands ticket, as customers are not permitted to lift floor tiles or access underfloor space.

4.4 Remote Hands

Remote Hands provides on-site support by Csquare personnel to customers within Csquare's data centers. Customers can request this service by submitting a Remote Hands ticket via the Customer Portal.

Remote Hands work, including work undertaken to assist a third-party, must be authorized through a Remote Hands support ticket. Csquare will not conduct Remote Hands activities for the customer or a third party unless authorized in a Remote Hands ticket.

The Remote Hands service is intended to provide basic functionality, as directed by the customer, at the customers own risk, and can be used to fulfill some of the following activities:

- Unpack and/or move small shipments to the customer cage
- Perform physical installation of equipment in a customer rack
- Reboot or power cycle equipment at customer direction
- Visual equipment checks, check for activity lights, link lights, etc.
- Attach a monitor, keyboard, mouse, or consoles to equipment
- Replace hot swappable customer hardware components with spares/upgrades
- Perform tape changes as instructed by the customer
- Move customer network cables between ports or interfaces as outlined by the customer
- Assist customer with troubleshooting and/or configuration via screen share
- Request an incoming shipment be unpacked and installed
- Change labeled cables
- Customer-approved escorts
- Load media (tapes, CDs, DVDs, or USB media)
- Execute built-in diagnostics according to customer instructions
- Perform other tasks requiring a similar skill level where immediate action is required

Activities considered out-of-scope for the Remote Hands service but not limited to:

- Any request for an add, change, or disconnect of **contracted services** (e.g. racks, cross-connects and power circuits) must be made through your account representative or ordered through the portal and not through a Remote Hands ticket
- Log into customer equipment without a screen share
- Replace non-hot swappable components or work that violates a manufacturer's warranty
- Run scripts or apply configuration changes to customer hardware without direct customer involvement
- Move heavy or oversized equipment

Remote Hands support tickets are handled based on priority definitions in Section 2.3 Support Priority Definitions. 48 hours' notice is required for engagements expected to last longer than two consecutive hours.

Csquare will update the Remote Hands ticket if additional information is required, and the Customer will receive automated reminders. If no response is received within seven days, Csquare may resolve the ticket. Resolved tickets will auto close after two days unless the Customer rejects the resolution in the Customer Portal, after which a new Remote Hands request must be submitted when the customer is ready to continue the engagement. Once a ticket is closed, the time worked will be billed on the following month's invoice.

Csquare may add billable time to a customer ticket if work is carried out on the customers' behalf, such as troubleshooting Csquare connectivity solutions resulting from customer misconfiguration, manual configuration changes such as BGP advertisements after initial installation, reporting and/or audit requests.

The initial time worked for each Remote Hands ticket submitted will be billed at a minimum of 60 minutes per Remote Hands ticket. Thereafter:

- The individual time worked for each activity needed to complete the Remote Hands request is calculated in 15-minute increments.
- Time worked for activities that require multiple technicians will be calculated by time taken for the activity multiplied by number of technicians for the activity.
- Materials are not included; however, materials may be requested via Remote Hands and may be available through Csquare's point-of-sale process.

Customers may purchase Remote Hands in the following ways:

- **On Demand**: Pay as you go with time worked invoiced the following month.
- **Subscription hours per month**: Package of Remote Hands hours billed as a month-to-month service.
    - Time worked for each Remote Hands ticket will be deducted against the subscription hours for that month.
    - A Remote Hands activity that exceeds the subscribed hours will be billed under the On-Demand Option. **Unused hours do not roll over to the following month.**
- For large complex engagements, please work with your account representative for a project-based quote vs. Remote Hands.

Scheduled Remote Hands

Remote Hands requests can be scheduled for a specific start time or a window of time from within the portal and require 48 hours advanced notice.

When scheduling a Remote Hands activity, the time entered will be the user's local time and once entered, the data center local time for the event will be displayed below it. Csquare may contact the requestor if it has a conflict with scheduling and suggest alternate times.

For scheduled Remote Hands, the start time of the scheduled window will be treated as the start time for the time worked, as resources must be scheduled to be available to start at the customer's requested start time.

Recurring Remote Hands

Customers can request a recurring Remote Hands activity to be set up by contacting Customer Care either by email, phone or submitting a "General Inquiry" / "Portal Question" ticket via the Customer Portal.

Recurring Remote Hands requests can be repeated daily, weekly (one or multiple days in the week), monthly, quarterly, or yearly. Typical recurring activities include regular tape swaps and audit requests.

4.4.1 Heavy or Oversized Equipment

Customers are responsible for moving fully or partially populated server racks and/or cabinets. Customers must consult with the relevant data center manager to coordinate the movement of this equipment. Customers must take care to consider the weight and size of the equipment to be moved, to ensure there will be no damage to the data center flooring. Customers will be held liable for any damage resulting from the movement of this equipment.

- Data center staff will not unload any racks, or customer owned equipment from trucks or move equipment greater than 300 pounds from the loading dock. Customers are responsible for organizing the moving and unpacking of equipment at their own expense.
- Installing or moving individual items of equipment over 50lbs into racks/cabinets requires more than one technician and the Remote Hands time worked will be calculated accordingly.
- Deliveries of over 300 pounds or taller than 84" must be discussed and approved by the data center staff and account team **prior** to shipment. Data centers may have height limits or require underfloor bracing (subject to additional charge).

4.5 Customer Packages and Shipments

Each of our facilities is equipped with a loading dock and storage areas for incoming and outgoing shipments. Csquare is not responsible for the logistics of shipments, and it is the customer's responsibility to organize all incoming and outgoing shipments and communicate with data center staff if required. Csquare will not organize shipping.

4.5.1 Incoming Shipments

All customer equipment brought to the Csquare data center must enter the facility through the shipping and receiving area.

- Csquare cannot be declared as Importer of Record for any shipments, and all duties and taxes must be pre-paid by the customer.
- Csquare does not accept mail/post on behalf of customers at the data center. All mail/post should be directed to the customer's business address.

All incoming shipments should be clearly labeled with the following information:

- Customer name and Colo ID c/o Csquare
- Csquare facility address
- Associated Csquare shipping ticket number
- Contact and phone number should be present on the packing note

Customers must create an incoming shipment ticket including tracking numbers for inbound shipments, ideally 24 hours before delivery of a shipment to a data center. Inbound shipment tickets can be created via the Customer Portal.

The customer is responsible for uncrating, unboxing, and transportation of equipment to the data center floor (no cardboard allowed) and any associated costs.

- Temporary access authorizations are required to authorize movers/carriers to access the data center and move equipment to the customers' colocation environment.
- Customers must remove all refuse (including, but not limited to boxes, crates, corrugated paper, plastic, and foam packing materials) from the shipping/receiving, hallways, customer lounges and common areas. Materials must be placed in a designated disposal area and marked as “trash”.
- Damaged deliveries:
    - Csquare will try to contact the customer on detection of a damaged delivery prior to acceptance.
    - If damage is detected during delivery, Csquare reserves the right to refuse delivery. If Csquare accepts delivery of a damaged package, it will endeavor to document the damage for the customer.

If customers need Csquare assistance with moving and installing deliveries to/from a cabinet or cage, they can create a Remote Hands ticket when creating an incoming shipment ticket.

- If a shipping ticket has already been created, then a separate Remote Hands ticket will need to be created. Comments added to a shipping ticket will not initiate a Remote Hands activity.
- Csquare reserves the right to refuse to move, unpack, or uncrate any customer materials, equipment, etc. for any reason including safety and liability concerns.
- The customer acknowledges that Csquare may discard the packaging as no cardboard is permitted on the raised floor, or at the customer’s request, store packaging in shared storage with the associated charges.
- If an incoming shipment has been received but the customer requires the delivery to be returned to the supplier, it is the customer’s responsibility to organize the return shipping and label the packages accordingly and Remote Hands charges will apply for any work undertaken by Csquare data center staff.

4.5.2 Unexpected or Unidentified Deliveries

If Csquare is not notified in advance of a shipment or the shipment is not clearly marked, Csquare reserves the right to refuse the delivery. Unexpected deliveries start incurring storage charges on the day of delivery with no complimentary storage period, and unidentified deliveries that have not been claimed within 90 days of arrival may be considered abandoned equipment.

- It is the customer’s responsibility to ensure vendors shipping to a data center on their behalf are correctly labeled with the customer’s name and Colo ID, and an expected delivery shipping ticket created.

4.5.3 Csquare Shared Storage

Csquare provides shared storage at data centers either in a shared storage room or on the loading dock, depending on availability and size of items/deliveries requiring storage.

Deliveries received by the data center are placed in shared storage and tracked at the individual package level. Customers may collect packages individually, with storage charges applying to individual packages not collected in a timely manner as described below.

Thirty days of complimentary storage (during which the customer is not charged for storage) is provided for inbound and outbound shipments for which Csquare has received notification prior to delivery and are correctly labeled displaying the company Colo ID and company name.

Complimentary storage does not apply to items already within the data center that the customer requests Csquare store on their behalf, items placed in storage for compliance issues or items left when a customer's colocation space is vacated. A shipping ticket is required for all items stored.

Shared storage fees are charged at a flat 30-day rate (no-prorating). Individual packages are assigned a "pickup before" date which is the expiration of complimentary storage or the previous 30 days paid storage.

If a delivery is not picked up by midnight on the day prior to the "pickup before" date, then a storage fee will be charged, and the customer will have another 30 days to pick up the delivery. Charges are correlated at the end of each month and invoiced on the customer's next Invoice. Midnight day of arrival is counted as day zero regardless of the time of arrival.

The customer assumes all risk of loss or damage to any customer equipment during the equipment storage period. Csquare reserves the right to treat packages as abandoned if storage charges are not paid. If any Customer Equipment remains in a Facility after fourteen (14) days following Csquare removal of Customer Equipment from the Equipment Space to storage, or Customer Equipment remains in storage after fourteen (14) days following the Date of Termination, then Customer agrees that the Customer Equipment shall be deemed to be transferred to Csquare, and Csquare may remove and dispose of the Customer Equipment at its sole discretion and may retain any proceeds from such disposition, without liability. Customer shall be responsible for any costs incurred by Csquare in taking any action pursuant to this Section

4.5.4 Outbound Shipments

The customer must ensure that shipping has been arranged with a carrier and the shipment is properly packaged, labeled, and an outbound shipping ticket has been created prior to the shipment being dropped off at the loading dock. The customer is responsible for making all arrangements with the shipping company.

Once the package is ready for shipment, customers must submit an outbound shipment request via the Customer Portal. Customers are required to schedule shipments with the carrier and complete all necessary paperwork for the shipment.

- Customers are required to pay shipping and insurance fees.
- A tracking number should be created with the customer's carrier prior to creating a Csquare shipping ticket or updated once the tracking number is established. The contact on the shipping case will be notified within 24 hours regarding any missing tracking numbers.
- The customer must provide their own packing material. Packaging material may be available onsite by contacting the data center staff, but use is at the customer's own risk.
- Csquare can assist in the packaging of shipments using Remote Hands but the liability for damage/loss to the packaged items remains with the customer.
- Csquare is not responsible for unattended shipments left in the lobby or loading dock area.

- Tape handling containers (i.e. Iron Mountain, Data Safe, Arsenal, etc.) are not permitted to be left unattended in the lobby or loading dock area.
- The customer must assign or request temporary access for their shipping company to enter their cage and/or cabinet.

5 Interconnection and Network Services

Csquare is a provider-neutral data center operator, in which a variety of network service providers can establish a presence within the facility and provide their services to Csquare colocation customers. Csquare colocation customers can establish low-latency connections between themselves or with other customers or providers.

For purposes of interconnection, Csquare operates meet me rooms in every facility. A meet-me room "(MMR)" is a designated space where telecommunications carriers, internet service providers, and data center customers interconnect their networks directly. Csquare's MMR serves as a central hub for physical network interconnections, allowing our customers to establish private, low-latency connections for data transmission without needing external cabling or third-party facilities.

Customers should confirm with Csquare first prior to ordering copper Ethernet connections to confirm that they do not exceed 100m/328ft.

5.1 Interconnection Offerings

Csquare's Interconnection portfolio encompasses a suite of products intended to satisfy the business needs for customers and service providers operating within Csquare facilities and data center markets. Please reach out to your Account Manager for specific questions on how to interconnect appropriately within a Csquare facility.

5.1.1 Ecosystem Connect

For all customers (including carriers and service providers) with colocation space within a Csquare data center, Ecosystem Connect provides pre-requisite connectivity to the MMR for the purpose of interconnection. Ecosystem Connect includes network patch panel(s), ports, and associated cabling to the nearest MMR. Ecosystem Connect panels are considered the demarcation for Csquare network and interconnection products. **See Section 6.5 Connectivity Policies**.

Customers can select from available Ecosystem Connect port bundles, and Csquare will install a multi-media capable patch panel(s) within the customer's colocation environment. For Secure Cabinet customers, the panel will be installed at the highest U position available unless otherwise specified by the customer. For Secure Cage customers, the customer should specify the rack and location where the panel should be deployed in their environment.

Csquare will install associated cabling which will be terminated to the back side of the panel.

- Customers are not permitted to adjust this cabling.
- If the customer causes damage to the panel, cabling, or associated ports, the customer is responsible for purchasing a replacement Ecosystem Connect panel and/or cabling.
- Connections from the front side of the Ecosystem Connect panel to customer equipment are the responsibility of the customer. The customer can request support from Csquare to complete these connections on their behalf via a Remote Hands ticket.

All Csquare cabling follows the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Cabling Standards 568B and 569B. Fiber cabling will be deployed as double-jacketed or armored as determined necessary by Csquare. Any deviation from these standards will require specific approval from Csquare prior to proceeding.

Below is current list of available Ecosystem Connect options at Csquare

Fiber (Single Mode and Multi-Mode)	**Copper (CAT6)**	**COAX**
6 Bundle Ecosystem Connect	6 Bundle Ecosystem Connect	3 Bundle Ecosystem Connect
12 Bundle Ecosystem Connect	12 Bundle Ecosystem Connect	
24 Bundle Ecosystem Connect		
48 Bundle Ecosystem Connect		

Note: For fiber Ecosystem Connect bundles, the quantity represents a fiber pair. For example, a 6 bundle of Ecosystem Connect will have 12 strands of fiber installed.

5.1.2 Cross Connect

A cross connect provides connectivity between the customer environment and a third-party within the Csquare data center. A cross connect is a cable that connects to two different Ecosystem Connect ports terminated within an MMR. Csquare offers the following cross connect options on a fixed term or month-to-month basis:

- Fiber Cross Connect
- Copper Cross Connect
- COAX Cross Connect
- Plain Old Telephone Service (POTS) Cross Connect

To support redundant cross connects, two separate Ecosystem Connect and cross connect services should be ordered. Csquare does not maintain a relationship between diverse Ecosystem Connect and/or cross connect installations and failover between the instances should be managed by the customer.

5.1.3 Riser Connect

Riser Connect is a dark fiber or copper connection that traverses from a Csquare data center to a different floor in the same building managed by a third-party data center provider (or another provider). Riser Connect allows access to a broader ecosystem of carriers and service providers in a multi-tenant data center facility. Note: POTS delivery over copper risers does not require the purchase of Riser Connect.

Standard delivery includes both the cross connect in the MMR and the non-Csquare (third-party) cross connect to the Z-end connection. Riser Connect service is terminated to a customer's Ecosystem Connect panel.

5.1.4 Intra Customer Connect

Intra Customer Connect provides a direct connection between two non-contiguous same-customer spaces within the same datacenter. Connections can be made directly within the same suite or may utilize Csquare facility fiber to complete connections. Intra Customer Connect cabling left coiled can be terminated to customer's equipment through Remote Hands.

The service only incurs an installation fee with no monthly recurring charge. Intra Customer Connect is not covered by the SLAs defined in the MSA. Customers wishing for SLAs must purchase Cross Connects.

5.1.5 Pathway

Pathway provides the ability for customers to connect their non-contiguous colocation environments in different Csquare data center buildings on the same campus. Csquare offers two variations of Pathway depending on customer needs:

- **Pathway Fiber:** fiber connectivity between Csquare facilities on a campus and is sold as single pairs of fiber up to a quantity of six over Csquare's campus network.
- **Pathway Conduit:** includes access to conduit, innerduct or Maxcell, in a larger conduit in which customers can run cabling of their choice between buildings. Customers may pull as much fiber through the size conduit ordered as will fit in the conduit, innerduct or Maxcell. Csquare does not control or limit in any way the use of the conduit access purchased by the customer.

Pathway construction will be completed by Csquare, and customers may not access Csquare-owned duct bank or complete any fiber pulls. Cabling is delivered to the customer's colocation environment and will be left coiled within the customer's designated cage or cabinet unless alternative termination instructions are agreed upon in the service order.

5.1.6 Metro Connect

Metro Connect service provides customers the ability to connect to their own environments or connect to a customer or service provider that is in another Csquare data center or third-party data center (where available) within the same metropolitan area. Metro connect is available in the following options:

- **Metro Connect Dedicated:** The Metro Connect Dedicated product utilizes Csquare's optical network to provide connectivity between the sites. Metro Connect Dedicated is available as a 10Gbps or 100Gbps WAVE service delivered over Csquare's optical network utilizing Ethernet Private Line protocol. Standard delivery provides single port and single path connectivity, and customers can select other options for redundancy for an additional fee.
- **Metro Connect Dark Fiber:** Metro Connect Dark Fiber is a single-mode fiber connection between a Csquare facility and another location within the same metropolitan area.

Available options for Metro Connect Dedicated include:

Service	Configuration	Failover	Available Speeds	Handoff Type
Metro Connect Dedicated	Single-threaded instance. No diversity.	None	10Gbps 100Gbps	Ethernet Private Line
Metro Connect Dedicated - single port / dual path	Two separate paths in a primary and secondary (active/passive) configuration.	Csquare managed	10Gbps 100Gbps	Ethernet Private Line

	Failover implemented via an Automatic Protection Switch (“APS”) in the event of a service disruption on either one of the paths.			
Metro Connect Dedicated - dual port / dual path	Two separate single threaded instances using separate ports and paths in a primary and secondary configuration (active/active).	Customer managed	10Gbps 100Gbps	Ethernet Private Line

Metro Connect service is delivered over single mode fiber with LC connectors and is terminated to the customer’s Ecosystem Connect panel.

5.1.7 Express Entrance

Express Entrance provides the ability for customers to connect into the Csquare data center from outside the Csquare managed space. Express Entrance is sold as either Express Entrance Conduit or Express Entrance - Fiber.

Customers may utilize Express Entrance in cases such as:

- Conduit access for fiber being deployed into the Csquare data center from a manhole on the street.
- Fiber deployed into the Csquare suite from another area not managed by Csquare within a multi-tenant building.
- Connecting an antenna deployed as part of Roof Rights.

Express Entrance – Conduit

Express Entrance - Conduit provides Csquare data center access or egress in support of cabling entering into the facility. Conduit associated with Express Entrance is deployed to house fiber or copper which is classified as either outside plant or inside plant.

- Outside Plant (OSP): Cabling from the manhole outside of the building.
- Inside Plant (ISP): Cabling from within the building, but outside the Csquare suite.

Customers may terminate cabling either directly to their colocation environment or to the MMR Terminations to the MMR require Ecosystem Entrance Panel. Note: Any cabling pulled into the Csquare data center is considered customer network, is not associated with Csquare network products and may not terminate to any gear associated with Csquare deployed network products such as Ecosystem Connect.

The deployment may be conduit, innerduct or Maxcell in a larger conduit and customers must contract installation services directly from Csquare.

Express Entrance – Fiber

Provides access to Csquare-owned single-mode fiber connecting a third-party provider location and the Csquare suite. The product is sold as single connections (a connection is composed of two fiber strands with LC connector) up to a quantity of six. For bundles larger than six, Csquare offers Express Entrance – Fiber (Custom Bundle) in which deployment specifications will be captured on the service order upon approval from Csquare.

Express Entrance – Fiber terminates within the MMR and is associated to ports on a Csquare panel. The applicable ports on the panel will be associated with the customer’s Express Entrance – Fiber and can be used to provide LOA/CFA for future cross connect ordering.

Cross connects in the third-party (non-Csquare area) are included with the product to complete the connection between the ordering party and the Csquare panel within the third-party area. Csquare will

order the third-party cross connects on behalf of the customer based on the LOA/CFA required to be provided by the customer defining the Z-end termination location within the 3rd party policy **See Section 6.5.4 Letter of Authorization (LOA/CFA) Policy**

5.1.8 Ecosystem Entrance Panel

The Ecosystem Entrance Panel is a passive panel in the MMR in which inbound cabling (fiber) may be terminated. This product is commonly ordered in conjunction with the Express Entrance product for the termination of dark fiber services. Ecosystem Entrance Panel ports can be provided on a Letter of Authorization/Customer Facility Assignment ("LOA/CFA") to Csquare customers for interconnection purposes.

5.2 On Demand Services

Csquare Digital Exchange™ is a software-defined network which virtually connects customers and services throughout the data center and metro region. This high availability architecture assures each customer's traffic is logically isolated and protected using the VXLAN protocol. Private virtual Layer 2 networks can be defined, provisioned, and configured through APIs or Customer Portal.

Csquare Digital Exchange™ is available in most data center locations today. Contact your account representative about specific availability.

5.2.1 Digital Exchange Port

All Csquare Digital Exchange™ services are accessed via the Digital Exchange Port service.

Customers can choose to utilize the full port for a single service or stack multiple services via the same interface. Customers can elect to purchase multiple Digital Exchange Ports to meet their specific needs and may aggregate multiple ports using the LAG protocol for ports configured as Layer 2 CE.

The Digital Exchange Port must be terminated to an Ecosystem Connect panel residing in the customer's colocation environment. The service is delivered over single-mode fiber (SMF) with LC connectors. Since the Digital Exchange Port service is redundant, the customer must have (2) available SMF ports on their Ecosystem Connect panel for connectivity. The service demarcation is at the Ecosystem Connect Panel and the point at which Csquare will provide end-to-end testing. All connections behind the Ecosystem Connect panel are considered the customer's network and are not included in end-to-end testing of network services sold to the customer.

The Digital Exchange Port has multiple configuration options, which are selected when activating the port from the portal or API. Customers should select the configuration option that matches their desired and/or existing network design. Available configuration options include Layer 3 CE, Layer 2, and Layer 2 CE with LAG.

A Digital Exchange Port includes:

- Cross Connects required from the Ecosystem Connect panel in the customer's colocation environment to the Csquare Digital Exchange™.
- Access to Csquare Digital Exchange™ enabled service providers via a Digital Cross Connect
- Access to Csquare Digital Exchange™ services such as IP Connect, Cloud Connect, and Metro-to-Metro Connect.

5.2.2 IP Connect

IP Connect provides colocation customers internet access service via a mix or "blend" of two or more upstream providers. Because of the blend of multiple providers, Csquare's IP Connect service provides additional redundancies to what is ordinarily provided by a traditional carrier internet service. IP Connect can be purchased via traditional physical interconnection or on-demand via Csquare Digital Exchange™.

IP Connect via Cross Connects

Csquare offers both dual and single port options to connect to the IP Connect service. Csquare recommends that customers purchase the dual port configuration for an additional layer of physical redundancy. Customers can select their media handoff as either copper with RJ45 connectors or single-mode fiber with LC connectors.

IP Connect bandwidth is sold in Committed Information Rate (CIR) tiers, and the customer can select for their service to be fixed or "burstable". Burstable configuration allows for the ability to exceed the committed information rate tier as needed. Burstable usage is billed monthly by calculating overage-based industry standard 95th Percentile (or 95th P) methodology multiplied by the contracted overage rate.

Several network configurations are available including Static, VRRP, and BGP. Some configurations may require the customer to manage failover, while others, Csquare manages failover. In addition, customers can lease IP address block(s) for use with the service, or the customer may choose to bring their own IPs for locations that support BGP routing.

Bursting capabilities are capped at the next bandwidth tier available of the IP Connect service.

IP Connect via Csquare Digital Exchange™

IP Connect services can also be delivered on-demand through Csquare Digital Exchange™ accessible through the Customer Portal. Customers must have an active Digital Exchange Port to purchase IP Connect via Csquare Digital Exchange™.

As a part of the order for IP Connect, customers must establish a Committed Information Rate ("CIR"), which represents the customer's committed bandwidth and sets the customers per megabit cost. Once a CIR is selected, the customer can choose for the service to be fixed or burstable.

Bursting capabilities are defined by customer's contracted CIR commitment tier and Digital Exchange Port service.

CIR	Exchange Port Type	Max Burst Bandwidth
0 - 999 Mbps	1,000 Mbps	1,000 Mbps
0 - 999 Mbps	10,000 Mbps	1,000 Mbps
1,000 Mbps	1,000 Mbps	1,000 Mbps
1,000-10,000 Mbps	10,000 Mbps	10,000 Mbps

During provisioning, customers can select configuration options such as BGP or Advanced Network Services depending on their requirements, at an additional cost.

- **Advanced Network Services (ANS):** provides additional Layer 3 network capabilities to IP Connect including Network Address Translation (NAT), Virtual Private Networking (VPN), and basic routing.
- **Border Gateway Protocol (BGP):** Customers wanting to advertise their own IPv4 or IPv6 public address space may choose to add a BGP service. Customers selecting BGP service must acknowledge ownership of the IP space they wish to use, which will be validated by Csquare prior to activation of the service. The minimum block Csquare will announce for IPv4 is a /24 and /48 for IPv6.

IP Addresses

IP Addresses can be leased from Csquare for use with the IP Connect service. Csquare offers IPV4 block and IPV6 options that can be made available at customer request.

Burst Measurement

For customers that select their IP Connect service to be “burstable”, overages charges are calculated based on the 95th P billing methodology. Bandwidth is measured (or sampled) from the Csquare router and recorded in a log file every five minutes (approximately 8,000 measurements per month). At the end of the month, the input samples are sorted from highest to lowest, and the top 5% of data are discarded (approximately 36 hours of a 30-day billing cycle). All values are rounded to the next highest whole number.

For example, if the 95th percentile value is 11.3Mbps, then the value considered is 12Mbps. The same is done with the output samples.

To arrive at the billable utilization for the month, Csquare selects the higher usage measurement of either the input or output traffic flow and calculates billing based on that usage measurement. Based on this model, the top 36 hours (top 5% of 720 hours) of peak traffic are not considered when billing for an entire month. Bandwidth could be utilized at a higher rate for up to 65 min a day with no financial impact on the monthly contracted commit. Overage is billed at the same per Mbps rate as the CIR multiplied by a 1.5 times escalator.

5.2.3 Digital Cross Connect

Digital Cross Connect service provides connectivity between the same or two different customers located in a Csquare data center, campus or metropolitan area and are both connected to the Csquare Digital Exchange™ via a Digital Exchange Port.

The bandwidth for Digital Cross Connect is capped at the minimum port speed on either side of the connection. For example, if the port on the originating side of the connection is a 1Gbps port and the port on the receiving side of the connection is 10 Gbps, the max throughput will be 1Gbps. Customers are required to manage actual throughput based on specific traffic being sent across the connection. Csquare will not cap or “throttle” any traffic across the connection beyond the minimum port speed.

Any Digital Cross Connect between different campuses in a metropolitan area is considered a Digital Metro Cross Connect and is subject to an additional fee.

5.2.4 Cloud Connect

Cloud Connect service provides secure, low latency layer 2 connectivity to public cloud providers through the Csquare Digital Exchange™. Customers must have an existing connection to the Csquare Digital Exchange™ through a Digital Exchange Port to consume this service. Bandwidth for Cloud Connect must be selected when provisioning the service. Customers must have an existing relationship with their desired cloud provider to utilize the service.

Path diversity requires separate physical connections to multiple Cloud Connects for different cloud service provider endpoints or regions. Customers can order multiple instances of Cloud Connects between the same or different points on the network, however Csquare views each order as a stand-alone instance and does not manage any failover scheme between Cloud Connects.

5.2.5 Metro-to-Metro Connect

Metro-to-Metro Connect services provide customers with the ability to connect multiple metropolitan regions together through Csquare Digital Exchange™. The Metro-to-Metro Connect service requires a

Digital Exchange Port service in both the originating and terminating locations of this service. Bandwidth for the Metro-to-Metro Connect must be selected when provisioning the service.

Path diversity requires separate physical connections to multiple Metro-to-Metro Connects for different endpoints or regions. Customers can order multiple instances of Metro-to-Metro between the same or different points on the network, however Csquare views each order as a stand-alone instance and does not manage any failover scheme between Metro to Metro Connect.

5.2.6 Hybrid Cross Connect

A Hybrid Cross Connect service connects customers in which only one customer is connected to the Csquare Digital Exchange™. The connection utilizes the customer's Digital Exchange Port to digitally connect to Csquare Digital Exchange Port in the MMR. From the Digital Exchange Port in the MMR, a physical cross connect will be connected to the Ecosystem Connect or Ecosystem Entrance panel of the Z-end customer. Once connection is in place, a VLAN must be established by the customer to direct traffic to the Z-end provider.

5.2.7 SmartCab

Csquare SmartCab allows customers to consume colocation with point-and-click provisioning of space and power with an integrated, configurable core network fabric.

Customers can dynamically configure and deploy their colocation on-demand via the Customer Portal. The SmartCab integrated network fabric connects to the Csquare Digital Exchange™ with pre-connected cabling to the Csquare Meet-Me-Room with the ability to interconnect with existing environments either within the same facility or other facilities in the Csquare global footprint via the Csquare Digital Exchange™.

Customers can physically access the SmartCab like standard colocation space, ship equipment to the data center and utilize Remote Hands to help install, configure customer equipment within the cabinet remotely.

SmartCab includes the following.

- Secure colocation space (1/4 Cabinet, ½ Cabinet, Full Cabinet)
    - Locking mechanism, either combo locks or electronic locks dependent on facility
    - Mounting rails
    - Redundant power feeds, 208v or 230v
    - Redundant power strips, non-metered, with C13 and C19 outlets
- (1) Single Mode Fiber 6 Bundle Ecosystem Connect for connectivity to the MMR
- Connectivity to Csquare Digital Exchange™ via a 2 RU patch panel installed in SmartCab environment. Dependent on SmartCab configuration, the customer will be provided with a mix of 10G fiber, 25G fiber, and 10baseT copper connections to Csquare Digital Exchange™.

6 Policies

Customers must comply with all Csquare rules and policies set out in this Customer Service Guide. If a customer fails to comply, Csquare reserves the right to take remedial action in relation to the failure, without prior notice to the customer.

6.1 Compliance, Reports and Audits

Csquare engages an external auditor to conduct annual audits of data center operations. The current audit reports and certificates are accessible on the Customer Portal for self-service, with compliance documents visible to all portal users. Access to these reports is governed by a non-disclosure agreement (NDA) included within each document. Typical documents available for download:

- Csquare SOC 1 Type II Report
- Csquare SOC 2 Type II Report
- SOC Bridge Letters
- Csquare PCI Attestation of Compliance (AOC) Report
- ISO 27001 Certificate and Statement of Applicability (SOA)
- NIST 800-83PE Attestation Letter
- Certificates of insurance

6.1.1 Additional Audit Requests

Customers can request additional reports, risk assessments, ESG/sustainability reports, audit details, or responses to questionnaires for information beyond what is included in Csquare's standard reports. To submit these requests, please use a Remote Hands ticket through the Customer Portal.

- Customers should provide a detailed list of audit/report items with their submission or tour request.
- Csquare's target response time for this type of request is 7-10 business days.
- Requests for Csquare proprietary information, including internal policies, system settings, and similar materials, must clearly specify the details in the request. Any proprietary information Csquare agrees to share will be accessible only in person at the relevant facility or through a scheduled virtual screen share. Csquare will not provide proprietary documents, screenshots, or other visual records, and customers are not permitted to photograph or capture this information in any way.
- For data center audit tours, customers must submit a tour request through the Customer Portal, specifying the purpose of the visit at least 30 days in advance. All attendees must be accompanied by a representative from the customer's team.

Csquare will apply the standard Remote Hands time worked policy to fulfill the request or supervise an auditor. Expedited requests will incur additional fees.

In addition to external compliance reports, the reports section in the Customer Portal offers a centralized location where customers can create and view and download a variety of reports. Customers can also set up automated reports to be generated on a daily, weekly, or monthly basis.

6.2 Data Center Policies

For the safety of our customers, visitors, and employees as well as the operational integrity of the data centers, Csquare has implemented a zero-tolerance policy within the data center for non-compliance to the policies outlined in this Customer Services Guide.

If a Customer is found to be out of compliance with the policies stated in this section, the customer must address any violations immediately.

- All SLAs are suspended until violations are remediated.
- Csquare may document the violation.
- For critical EH&S (Environmental Health and Safety) issues, Csquare may remediate immediately and then provide notification to the customer.
- Csquare regards customer breach of Csquare policy as a material breach of contract and Csquare reserves the right to suspend and/or terminate the services because of such breach.

If not remedied within the timeline given in the violation notice, Csquare has the right to implement the following with no liability for loss of Customer service.

- Csquare personnel will remediate the violation and charge the customer for the Remote Hands time taken (rounded up to the next hour).
- Place unracked or incorrectly stored equipment in storage (storage is billable along with the Remote Hands time to store the equipment).
- Charge for any damage caused to the colocation environment or cost of equipment disposal.
- Csquare reserves the right to remove any non-compliant cabling from the customer's environment.

6.2.1 Physical Access Policy

Visitors must only access authorized areas within the data center, such as lobby, customer lounge, conference rooms, public areas, and customer's own space on the data center floor.

- CCTV is in operation throughout the facility, and all visitors entering the facility agree to such surveillance.
- All visitors must enter and exit the facility via the mantraps / main lobby. Emergency, loading dock or service exits are to only be used in a fire or life safety emergency.
- Customers must not allow any unauthorized persons to access the data center (e.g., by "tailgating" or other means). Tailgating is defined as the practice of one individual entering the data center or colocation area by following behind another individual with badge access.
- Interior or exterior data center doors may not be propped open at any time.
- Unescorted access to unauthorized areas of the data center is strictly prohibited. Visitors may only access those portions of the data center made available by Csquare to customers for the placement of their equipment and use of the data center services, and common areas.

Tailgating and accessing unauthorized areas while unescorted will result in permanent ban to all Csquare locations.

6.2.2 Visitor Policy

Csquare's data center policies apply to all visitors, including any contact (third-party, vendor, etc.) authorized by a Csquare customer to access their environment. Customers must cooperate with and

comply with all reasonable requests of data center personnel while in the facility, including immediately addressing any policy violations when brought to the customer's attention.

The following applies to any visitor to a Csquare data center.

- All visitors to the data center must wear appropriate attire; that will not be deemed offensive by other visitors or staff at the data center.
- Smoking (including electronic cigarettes) is prohibited on Csquare property.
- Animals, except for service dogs, are not allowed within any area of the data center.
- Persons under 18 years of age require adult supervision and are not permitted within the Data center without the express written permission of Csquare.
- Customers/visitors must not harass or interfere with the activities of any individual within the data center, including any employees or representatives of Csquare or other customers.
- Customers/visitors may not engage in any activity that is in violation of law, or the Csquare Acceptable Use Policy found in this document.
- Comply with access policies implemented by Csquare in the event of government-issued emergency orders or to comply with public health advisories.
- Customers/Visitors may not use, touch, inspect, or otherwise interface with any Csquare or third-party property or equipment.
- Csquare may use temporary safety cones, barricades, or other safety devices to direct people away from hazardous areas. These locations are off limits to customers.
- It is the Customer's responsibility to provide for its Customer Representative's hearing protection if they access areas of the data center that have noise levels that exceed a regulatory action level.
- Customers/visitors are expected to be familiar with and adhere to all OSHA standards associated with working in a computer room environment.

A visitor's failure to adhere to Csquare's safety policies will result in expulsion from our data centers. Csquare may, at its discretion and at any time, revoke access privileges for any visitor.

6.2.3 Evacuation Policy

In an emergency, visitors must immediately evacuate the data center. Emergency procedures are posted throughout the data centers and exits labeled. Visitors unable to locate an evacuation plan can ask the data center staff for assistance.

All customers are required to follow verbal instructions provided by the data center staff. Customers must remain outside the Facility until they receive instructions from data center staff, or the local authorities. In no event should customers remain in a location that is unsafe.

6.2.4 Prohibited Materials

All containers, packages, boxes, bags, briefcases, purses, backpacks, and equipment carried into or out of the data center are subject to inspection by security and/or data center staff. If prohibited items are discovered, the individual may be denied entry. The following items are prohibited in Csquare data centers:

- Csquare strictly prohibits firearms and other types of weapons, including, but not limited to, knives, explosives (including fireworks), chemicals or other substances, and/or hazardous devices in its data centers. Employees, contractors, customers, and visitors are required to lock weapons safely in their personal vehicle before entering the premises
- Hazardous materials or other chemicals

- Equipment that could cause smoke, metal filings or shavings, heat, or particulates (e.g., power tools, torches, soldering or welding equipment)
- Alcohol, illegal drugs, as well as other intoxicants
- Magnets and electromagnetic devices
- Radioactive materials
- Muddy footwear or outerwear that could contaminate the colocation environment
- Motorized equipment/vehicles of any type are prohibited in the data center unless they are required for physical or medical purposes
- UPS equipment or backup battery systems of any type, other than what is provided by Csquare

6.2.5 Raised Floor Policy

The following are prohibited from any area of the raised floor including customer colocation environments.

- Eating and drinking are only permitted within the common areas of the data center; no food or drink is allowed.
- Wood, wooden pallets, other crating material, cardboard, boxes, paper products (other than equipment manuals), or other combustible materials of any kind.
- Liquids, unless authorized by Csquare as part of a liquid cooling solution.
- Fans and heaters

6.2.6 Video and Photo Recording Policy

Customers may only take close up pictures of their own equipment to record serial numbers etc. within their own colocation environment and must not have any other customers' environment within the frame. Customers must not take other pictures or recordings of any type on the data center premises unless specific approvals are received as described below.

Customers can request a limited exception to take wider angle pictures or video of their own equipment, by creating a "customer assist - Remote Hands" ticket within the Customer Portal a minimum of 24 hours in advance, specifying the Colo ID to be photographed, and the date and time. This is classified as an escorted event and will be charged under Remote Hands.

Csquare data center staff will supervise the session and review photographs and/or recordings to ensure compliance with this policy. Any photographs or recordings out of compliance must be deleted immediately.

6.2.7 Common Area Connectivity Policy

Csquare may provide network, Wi-Fi and phone services for visitors to use within the data center. Csquare wireless and wired access in common areas is purely for temporary connection of mobile devices and laptops while the visitor is onsite and is not to be used for internet connectivity for customer colocation equipment. By using these services, a visitor agrees to Csquare's acceptable use policy **Section 6.5.6 Acceptable Use Policy**.

6.3 Colocation Environment Policies

Cabinet arrangements within the cage are determined by Csquare and are not subject to change without consulting Csquare personnel. Cabinets within the cage may be provided by Csquare, or provided by the customer, but must be installed and anchored by Csquare personnel or Csquare authorized contractors.

Customers are not permitted to alter, change, or install any locking mechanism on their space, except for a cabinet lock combination code. Customers are not permitted to alter or change any Csquare provided cabinet or rack. This includes, but is not limited to, removal of doors, drilling holes, or mounting equipment to the exterior of the cabinet or rack. All customer equipment must fit in the cage or cabinet provided by Csquare so that the cage or cabinet can be secured in a locked position.

Customer space shall not pose any danger or hazard to anyone in the data center. Customers are prohibited from engaging in any activities or actions that may adversely affect neighboring customer environments and/or the efficient operation of the site.

- Customers must keep their area clean at all times. Cages must be free of debris.
- No combustible material (e.g., wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids, or solvents, etc.) may be present in a customer's cabinet or cage.
- Customers may not climb onto cabinets or scale cage walls. Customers must request data center staff assistance if needing to access cabinet/rack tops.
- Customers may not make physical alterations or modifications to the space without prior written permission from Csquare.
- Unused cabling must be stored out of sight and equipment stored without impeding airflow.
- Customers must not block egress routes/aisleways while moving equipment into or out of a cage.
- Customers may use the open space in their cage as a temporary staging area for equipment but must ensure that all equipment is properly mounted in cabinets prior to leaving the site. Live equipment must be properly mounted in cabinets and cannot be left on the floor.

Customers are expected to comply with airflow markings and mount equipment according to the cold-aisle/hot-aisle designations.

- All equipment placed in any data center must vent the heat directly into the hot aisle where it is then contained and prevent it from mixing back into the cold aisle.
- Customers must obtain approval from Csquare with regards to hot and cold aisle layout configuration prior to equipment installation and must adhere to the approved configuration and any requirements specified by Csquare in its approval.
- Customers who have solutions that require additional environmental management configurations including but not limited to venting, additional containment or alternatives to air cooling must obtain prior approval from Csquare. Csquare reserves the right to charge customers additional set-up fees in connection with additional environmental management configurations as deemed necessary.
- Open spaces in the cabinet must be covered with blanking panels to ensure proper airflow pressure is maintained. Csquare may provide up to ten complimentary blanking panels per rack, subject to availability. Csquare may conduct periodic compliance audits to ensure customers are maintaining proper blanking panel installation within cabinet environments and may require customers to close any open U-space with blanking panel(s) within five (5) business days of notification.
- Customers must keep tile vents clear of any obstruction. Customers are not permitted to lift floor tiles or open underfloor space under any circumstances. If access is necessary during installation, customers may open a Remote Hands to request data center staff make any adjustments

Except for reasonable wear and tear, Customer agrees to maintain and return the Equipment Space in an orderly and safe condition following the termination of Customer’s space-related Services. Failure to do so may result in Csquare cleaning the Equipment Space and passing the costs on to Customer. If Customer fails to remove Customer Equipment, vacate the Facility, or continues to draw power on the Date of Termination, such Date of Termination shall void. Customer must issue a new notice of termination in accordance with this Agreement to Csquare and Csquare will continue to bill under existing rates.

6.3.1 Customer Equipment

Customer cabinets and cages must always be maintained in a clean, neat, and orderly manner.

- Customer equipment must comply with all applicable manufacturer specifications, regulations, and industry standards, including those relating to proper installation, power consumption, and ventilation/heat dissipation.
- All customer-provided equipment deployed in racks or cabinets within the customer environment must be UL (Underwriters Laboratory) listed or comply with other such local or regional certification programs providing equivalent levels of certification for such equipment.
- Customer equipment must comply with all applicable electrical codes.
- All equipment must be mounted within a rack; operating unmounted equipment is strictly prohibited.
- Equipment may NOT be stored/stacked on the floor in the customer space.
- Heavy or deep equipment mounted in racks or cabinets must also be supported by rear mounts or mounted on a shelf to prevent damage to the rack mounting rails.
- All spare equipment shall be mounted in a cabinet or kept in approved containers.
- Customers are strongly encouraged to label and/or tag all equipment and connections within their cage if they anticipate needing Remote Hands to assist with managing the contents of their cage.

Customers are responsible for providing their own tools and equipment. Portable carts/trolleys for moving small items and portable monitor stands may be available for use in all data centers. Csquare may loan equipment and tools to customers solely at the customer's own risk. Csquare is not responsible for any injury, loss or damage resulting from the customer's use of such tools or equipment.

6.3.2 In-Cage Storage

Customers are required to maintain their cage or cabinet in a neat and orderly fashion.

- Customers must not hang or mount anything on the cage mesh walls or cabinets.
- The creation of "office space" within the customer's cage or vicinity is prohibited. Small metal tables and chairs are permissible for short-term use but must be kept clear of cage doors, airflow systems, and walkways while not in use.
- The top of a cabinet, ladder rack, or enclosed cage may not be used for physical storage.

With Csquare permission, a limited number of approved containers may be used within a customer's cage, solely to store tools and cables etc., and not for the storage of rack mount or bulky equipment.

- Containers must not take up significant space, nor be stacked or positioned so as to obstruct physical access or airflow within the cage.
- Storage containers must be sealed when not in use.
- Csquare requires customers to use fire-rated containers for storage within a cage.

Data centers have storage lockers or dedicated storage space available to rent for a customer's exclusive use. Customers can contact their account representative to discuss availability and pricing.

6.3.3 Customer Cabling

For any cabling needs within a customer environment, customers must implement cabling that meets the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) standards of 568

and 569. Csquare offers structured cabling services in all data centers if requested. Customers can contact their account representative for more information.

- Cabling must not obstruct airflow/ventilation (such as perforated tiles) or access to power strips.
- All devices and cabling should be clearly labeled in a unique naming fashion.
- Cable wrapping, wire management, zip ties and/or Velcro must be used to organize cabling in a rack or cabinet.
- Unsecured cabling across aisles, on the floor, or around cabinet doors is strictly prohibited.
- Customers must properly run and secure cables within cabinets by using approved overhead and vertical cable management devices. Customers must install cabling in a safe manner so that it in no way impedes aisles, floor, or entranceways nor presents a fire hazard.
- Customers are not permitted to modify or change Csquare's cable management on the Csquare side of the demarcation panel.

6.3.4 In-Cage Security Equipment

Customers may install sensors and webcams within their environment provided they do not physically damage cabinets or cages. Customers must obtain prior approval from Csquare via a Remote Hands ticket.

Customers are not permitted to add security devices that would hinder Csquare's access to the cage or cabinet. Csquare personnel must always retain access to all areas of the data center.

- Customers must obtain Csquare's prior written consent in relation to the design and installation of, and any changes to, customer security systems.
    - Equipment will not be connected to the Csquare surveillance systems or block / interfere with any Csquare surveillance equipment.
    - Sensors and cameras may not be attached to the cage itself, and their position must be approved by data center staff **prior** to installation.
    - Equipment must be securely installed to assure that it does not present a safety issue (falling, head injuries, etc.).
- Customers accept all responsibility for monitoring and maintaining their video surveillance equipment. Csquare will not proactively monitor, nor respond to customer-owned video surveillance equipment alarms or service issues related to the video surveillance equipment.
    - Customer webcams must be fixed-mount with no pan-tilt-zoom capabilities, and the field of view limited to the customer's cage space only.
    - Customers must provide the proposed floor plan with camera positioning and approximate camera view angle. Customers represent that they have provided all necessary privacy notices and obtained all necessary consents when installing and using any video surveillance equipment.
    - Cameras may be placed facing the door of the customer's cage, but the customer must request, at their expense, opaque panels be installed to obscure outside the cage.
    - Csquare personnel must review the field of view of all customer cameras and reserve the right to disable and/or mask any cameras that are in violation of the policy.
- Sound recording devices, including webcam audio, are not permitted within the data center.
- Unapproved use of sirens and strobe lights is strictly prohibited.

6.3.5 Customer Environmental Monitoring

Customers may install environmental sensing devices in their cage or cabinet; however, any readings derived from customer-installed sensors will be considered secondary to Csquare's environmental monitoring and are not subject to service level agreement (SLA).

6.3.6 Customer Wireless Access Points (WAP)

Customers may install wireless access points, but only within their own cage environment. The customer must adhere to the following:

- Wireless devices may not interfere with or block any other wireless signals or electronics within the facility and must comply with relevant security standards, where applicable.
- Placement of all devices, including but not limited to wireless access points and antennas, must remain within the customer's site footprint and may not be secured to the cage itself.
- Csquare has no obligation to install or support customer devices or to respond to any repairs, maintenance, or distress calls regarding the devices, and is not responsible for any damage or loss of devices.
- Customers must immediately rectify or disable any wireless devices upon notification by data center staff of compliance issues.
- The use of customer wireless access points is used at the customer's own risk.

6.3.7 Customer Signage

Customer signage in the data center is prohibited. Posters or material should not be attached to the cage walls and should not contain content that could be deemed offensive by other visitors or staff at the data center.

6.3.8 Environmental Equipment Disposal

Customers are responsible for the proper disposal of their property, including electronic equipment, in accordance with any national or local laws and regulations.

- Recycling, destruction, and/or electronic waste (e-waste) handling must be arranged appropriately by the customer.
- Csquare encourages our customers who must dispose of electronic equipment (e-waste) to utilize a certified e-waste recycling service.
- Customer-owned electronic equipment (including power supplies, circuit cards, etc.) may not be deposited in a Csquare trash receptacle.
- If loading dock access is necessary for equipment disposal, a Remote Hands ticket must be made online to request assistance and supervised access as required by Csquare. Customers must submit an outbound shipment request if they need Csquare to stage equipment for disposal.

6.4 Data Center Power Policy

Contracted Power

Contracted Power is the total Maximum Active Power in kW that a customer is contracted to (draw) for a cage or cabinet.

Customers must not exceed their contracted power.

- Customers wishing to increase their contracted power must contact their Csquare account representative and increase their contracted kW prior to drawing active power above their contracted power.
- Csquare will conduct periodic audits to ensure compliance.

If a customer exceeds their contracted power allocation in a particular cage/cabinet, Csquare will charge the customer for excess power usage at 150% of the customers' current kW rate through the end of the current service term. Customers that continue to exceed their contracted power will be charged to increase their contracted power to accommodate the additional usage at current prices to the end of the current term. For the avoidance of doubt, this provision also applies to metered power colocation environments (including metered power cabinets).

Provisioned Apparent Power ("PAP")

Each circuit has a maximum total power (kVA) calculated by multiplying the voltage (V) of the circuit by the amps (A) of the circuit, multiplied by 1.73 if the circuit is a three-phase circuit.

- Single phase: amps x volts
- Three phase: amps x volts x 1.73

PAP is the breaker load for the given circuit, and if active power (draw) exceeds PAP then the breaker will trip isolating power from the circuit.

To ensure customer uptime, power distribution (power circuits or whips) will be provisioned in a redundant fashion unless non-redundant circuits are expressly requested. Provisioned apparent power is to be maintained at a quantity not to exceed 150% of the customer's contracted power. Customers having or desiring distribution of provisioned apparent power more than 150% of contracted power will be charged a monthly recurring fee for each additional circuit. Standard non-recurring charges apply. Paying for additional power distribution does not provide an exception to exceeding overall contracted power.

Maximum Active Power ("MAP")

Maximum active power (kW) is the maximum amount of power a customer is allowed to draw from a specific circuit. Exceeding MAP is against Csquare policy, National Electrical Code, and risks tripping the circuit breaker.

Customers must not exceed maximum active power of the provisioned apparent power for any specific circuit/circuit pair.

- Maximum active power is calculated based on an 80% power factor (PF) of the provisioned apparent power for a specific circuit/circuit pair.
- Csquare power service level agreements (SLAs) are not applicable if a customer exceeds the maximum active power for a given circuit/circuit pair or improper load distribution.

Csquare's power SLA does not cover circuit overloads caused by improper IT Load distribution. The combined draw on the A and B side of any circuit must not exceed the MAP for that circuit. **See Section 4.3.1 Power Distribution and Circuit Ratings.** Customers that exceed the maximum active power on an A and B circuit pair will be required to redistribute their active power to alternative circuits or purchase additional circuits.

Powering Equipment

Standard power circuits are delivered either in a single or redundant configuration (A-side and a B-side) are available.

- If single-corded IT equipment is unavoidable, Csquare may support the use of in-rack transfer switches on an individual case basis upon review but will not offer SLA credits for use of such equipment.
- Power audits for non-metered power circuits can be requested by creating a Remote Hands ticket with the subcategory "audits (power, general other)" and will be billed at the standard Remote Hands rate.
- The use of Y-cables, piggy-back PDUs, or daisy-chaining power strips is strictly prohibited.
- All equipment must be powered from circuits terminated in the same cabinet.

- Any mechanism or device that results in an increase in the outlet density within a rack beyond the intended 1:1 relationship between a single rack PDU and an individual power circuit is prohibited.
- Customers are expected to use the power provided to support customary IT loads. Cabinet power circuits should not be used for permanent or semi-permanent non-IT loads, such as tools, appliances, fans, heaters, etc.
- If a customer requires circuits for permanent or semi-permanent non-IT loads, they can request a non-redundant 120V circuit to be installed for a fee.
- Use of Csquare janitorial / non-IT loads power outlets is prohibited for customers
- The use of UPS equipment, including batteries or transformers, in customer space is strictly prohibited.
- Csquare reserves the right to deny customers the use of power transfer devices that may compromise the integrity of the power distribution network.

6.5 Connectivity Policies

The following policies are related to connectivity services provided by Csquare.

6.5.1 Media Converters and/or Extension Networks

If a copper cross connect cannot be deployed due to distance limitations, Csquare will reject the order and require a fiber cross connect order to be placed instead. Any media conversion is the customer's responsibility within their environment.

6.5.2 Meet-Me-Room Access

To maintain a secure environment for interconnection, all access to MMRs is limited to Csquare personnel.

No customer equipment will be co-located within MMRs.

- In instances where customer equipment is already installed in an MMR, Csquare will allow the equipment to remain. However, if at any time the customer requests additional power or other infrastructure changes to their environment that is located within an MMR, they will be required to move to a cage or cabinet on the data center floor.
  - If the customer requires access to equipment located in the MMR, they must open a Remote Hands ticket and a Csquare employee will escort them for the duration they are within the MMR. The escorted time will be billable to the customer.

6.5.3 Meet-Me-Room Interconnectivity

Csquare follows a one meet-me-room policy. Customer environments will be connected to the closest MMR in the facility via the Ecosystem Connect product.

- Connectivity between MMRs is provided via copper, single mode and multi-mode fiber managed and maintained by Csquare.
- If a fiber cross connect is required to terminate to another MMR within the facility, Csquare will design the connection to traverse the fiber backhaul network between the MMRs.
- If a POTS or T1 cross connect is required, Csquare will use the copper connectivity between MMRs to complete the connection.
- Copper ethernet and Coax cross connects are not able to traverse multiple MMRs due to distance limitations.

6.5.4 Letter of Authorization (LOA/CFA) Policy

Letter of Authorization (“LOA”) is a term used to describe an official letter that provides written authorization to connect to other parties within a data center and includes information about where a circuit should be terminated to a telecommunications carrier or other Z-end parties interconnection environment.

The connecting information provided on the LOA is commonly referred to as connecting facility assignment (“CFA”). The CFA is also sometimes referred to as carrier, customer, or circuit facility assignment. The CFA includes specific information on the location where the data center operator is to terminate a connection on the non-ordering (Z-end) customer’s demarcation point (“DMARC”).

Csquare Interconnection Policy

Csquare operates in two primary locations for interconnection. The MMR and the Csquare Telco Room (“CTR”). The MMR is the primary interconnection point for customers connecting to each other within the Csquare facility. The CTR provides the primary location for interconnecting to local exchange POTS line services; however, the LEC may choose to extend POTS lines to the MMR for interconnection with data center ecosystem members.

Acceptable Demarcation Points

All connections between ecosystem members within a Csquare data center (whether an enterprise, carrier or other service provider) must occur in the MMR unless otherwise noted in the product description for the product. Acceptable connection points for Csquare network products are to a Csquare network panel (typically deployed with Ecosystem Connect or Ecosystem Entrance Panel) for both the A-end (the ordering customer) and Z-end sides of the connection. All LOA/CFAs provided for Csquare network products should define the port on the Csquare network panel to be used for the connection. Any LOA/CFA defining the termination point as directly to a customer device will not be accepted.

POTS cross connects may terminate to either a telco block (66 block, 110 block) in the MMR, CTR or to a Csquare network panel. In all cases, a CFA is required to note the phone number of the POTS line and any additional information regarding the demarcation point as provided by the LEC. An official letterhead LOA is highly preferred but not required for POTS lines.

For connections terminating to locations outside the Csquare data center, the LOA/CFA should indicate the exact handoff location or demarcation point where the circuit is located within non-

Csquare location. Csquare will order the cross connect from Csquare’s termination point in the non-Csquare location to the Z-end customer based on the provided LOA/CFA.

Customers providing LOA/CFA to Csquare

Customers must supply LOA/CFA at the time of ordering any product that requires LOA/CFA. Csquare will not install any interconnection product that requires LOA/CFA without a properly completed LOA/CFA. Csquare will place orders on hold until the customer can obtain and provide the proper documentation for the order to proceed.

If LOA/CFA is not supplied within a reasonable amount of time, the order may be subject to cancellation.

- A LOA/CFA must be uploaded with the Portal order submission. Portal orders may not be submitted without an attached LOA/CFA. If the LOA/CFA is incomplete or contains an error, the order will not be accepted by Csquare.
- The customer will be given three business days to provide a corrected LOA/CFA.
- Csquare will allow the customer two attempts, each with three business days to cure.

- After two attempts, Csquare reserves the right to cancel the order. If a paper order is required, cross connects can be ordered via the Csquare Account team, but delays in delivering the service may be experienced.

Please work with the service delivery representative assigned to the order to avoid order cancellation. The representative will be able to assist with questions or coordination if you are having difficulty obtaining LOA/CFA or have questions regarding the elements required to be defined on the LOA/CFA.

Csquare providing LOA/CFA to Customers

Csquare does not provide LOA/CFA to customers as Csquare is responsible, in all cases, for the termination of all Z-end demarcation points as outlined in the service descriptions for products providing connections to Z-end parties.

6.5.5 Denial of Service

If a denial-of-service attack is detected on an on-demand service that has the potential to impact other customers, Csquare reserves the right to initiate Remotely Triggered Black Hole (RTBH) routing to mitigate the attack. Csquare reserves the right to leave the impacted service in RTBH state for as long as considered technically necessary to preserve the integrity of the network.

6.5.6 Acceptable Use Policy

To use any or all Csquare services a customer agrees to be bound to the Csquare Acceptable Use Policy. This Acceptable Use Policy (“AUP") for Csquare services is designed to help protect you, Csquare, its customers, and the Internet community in general from fraud, abuse of resources, and irresponsible or illegal activities.

Customer Responsibilities

Customer is responsible for the activities of its personnel, customers or end-users, by accepting service from Csquare, agrees to inform its customers and/or end-users of this AUP or its own Acceptable Use Policy, which must be co-extensive and consistent with these terms.

Prohibited Conduct

Services may only be used for lawful and appropriate purposes. Customers may not transmit, retransmit, redirect, or store material in violation of Federal or state laws or regulations, industry, or community standards, including, but not limited to, obscenity, indecency, defamatory or material infringing trademarks or copyrights. Csquare customers may not abuse or fraudulently use services, nor allow such use by others. The following illustrates some, but not all, uses that are prohibited under this AUP:

(1) Child Pornography: It is illegal under federal child exploitation statutes to possess, produce, receive, transport, or distribute by any means, including computer, visual depictions of "sexual intercourse" and/or "sexually explicit conduct" involving persons under the age of 18.

(2) Inappropriate Content: Using the services to transmit, distribute, redirect, or store material that, as reasonably determined by Csquare, is inappropriate, obscene, defamatory, libelous, threatening, abusive, hateful or which contains or incites violence.

(3) Denial of Service: Engaging in activity that may or will interfere with the service of another user, host, or network on the Internet. Users are also prohibited from activity considered a precursor to attempted security violations including, but not limited to, any form of scanning, probing, or other testing or information gathering activity, without prior express written consent from Csquare.

(4) Distribution of Viruses: Distribution of software, programs or messages that may cause damage or annoyance to persons, data, and/or computer systems. Hosts not timely secured or removed by customers may be blocked by Csquare from accessing Csquare services.

(5) Forging Headers: Forging or misrepresenting a message header of an electronic transmission originating or passing through Csquare services.

(6) Email Spamming [or Mailbombing]: The transmitting of unsolicited email to multiple recipients, sending large amounts of email repeatedly that annoys, harasses, or threatens another person or entity, or attempts to use services for SPAM. Sending unsolicited bulk email from another Internet service provider's network advertising or implicating any service hosted or provided by Csquare, including without limitation email, web hosting, FTP and DNS services. The sending of email with added words/characters to bypass Bayesian filters is prohibited. For bulk emailers, removal of complainants is required, as is the creation of a master no-send list. Bulk emailers may also be required to provide the complete confirmed opt-in information for each complainant within 24 hours of the request. Bulk emailers will also be required to demonstrate a definitive prior business relationship between the sender and the recipient. Utilizing a customer affiliate program to generate leads makes the customer responsible for the actions of its affiliates. This control includes, but is not limited to, blocking affiliate links and sending the affiliate traffic to a 404-error type page.

(7) Fraudulent Activities: Fraudulent activities including, but not limited to, intentional misrepresentations or misleading statements, writings or activities made with the intent that the person receiving it will act upon it; obtaining services with the intent to avoid payment; and hosting of phishing websites.

(8) Unauthorized Access: Unauthorized access includes the illegal or unauthorized access to other computers, accounts, or networks; accessing or attempting to access computer resources belonging to another party; attempting to penetrate security measures of other systems; using services not included in customer's contract; devising ways to circumvent security in order to access unsubscribed services; using the services in a manner that encumbers disk space, processors or other system resources beyond amounts allowed by the specific type of product; and/or interfering with a service, overloading a service or attempting to disable a host not assigned to customer.

(9) Network Sabotage: Use of services in a manner that interferes with others' use of the Internet or Csquare's network.

(10) Pyramid Schemes: Use of a fraudulent system of achieving financial gain, which requires an endless stream of recruits for success.

(11) Unlawful Acts: Use of services to violate the law or in aid of any unlawful act.

(12) Non-email Based Spamming: Posting of messages to newsgroups/blogs/services that are irrelevant, blanket posting of messages to multiple newsgroups/blogs/services, and the posting of annoying, harassing and/or threatening messages. Violation of any rules, policies or charters posted online by any search engine, subscription web service, chat area, bulletin board, webpage, or any other service accessed via Csquare services is prohibited.

(13) Facilitating a Violation of this AUP: Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to allow a user to violate this AUP. This includes, but is not limited to, the facilitation of the means to spam, initiation of pinging, flooding, mail bombing, denial of service attacks, and piracy of software.

(14) Blacklisting: Behavior by a customer that causes blacklisting must be remedied within 48 hours of written, electronic, or telephonic notice from Csquare. Activities that result in re-listing are prohibited and must be stopped immediately. Known spammers, previously unidentified, will be removed from the network once identified.

Violations and Enforcement

Violations will be enforced in accordance with the MSA.

6.6 Month-to-Month Services

Month-to-month services are services provided on a limited one-month term. Unless otherwise specified in the Service Order or Customer Portal order, including but not limited to, the following services are provided on a month-to-month basis. Month-to-month Services incur a monthly recurring charge, billed one month in advance.

- Cross Connect
- Riser Connect
- Digital Exchange Port
- IP Connect
- Cloud Connect
- Metro to Metro Connect
- Hybrid Cross Connect
- Digital Cross Connect

Services installed and utilized by a customer are considered accepted by the customer under the terms of the MSA. If the Services are not reflected in a Service Order but the customer is utilizing them, Csquare may bill those Services at the then-current rate.

Month-to-month services may be cancelled by either party by providing at least 30 days' advance written notice of cancellation to the other party. Month-to-month services are not prorated and will be billed through the end of the month following the month of the notice period expiration. Csquare reserves the right to adjust the charges for month-to-month services by providing customers with at least 30 days' advance notice of such adjustment.

Customers who have legacy Dual Site Cross Connect service in which the carrier and carrier's customer are both responsible for a portion of the overall connection, require additional documentation to prevent a potential service impact. Carriers wishing to disconnect a Dual Site Cross Connect will be required to obtain a disconnect acknowledgement from their customer and submit the form with their disconnect order before Csquare will process the request. Contact a Csquare account representative for a copy of the Disconnect Acknowledgement Form.

7 Business Continuity

This section provides an overview of Csquare's business continuity and disaster recovery plan ("BCDR Plan"). Csquare's Business Continuity and Disaster Recovery Team ensures that our services are prepared for and able to rapidly respond to any event that could impact business operations. This requires assessing Csquare's current emergency frameworks and advancing them to address gaps and create standards that will bolster Csquare's resiliency and mitigate risks to our operations.

Through a top-down approach, Csquare's Business Continuity and Disaster Recovery Team strengthens our current emergency frameworks to adapt to the world's changing natural, human-caused, and technological threat landscape. To preserve confidentiality and security, this overview provides illustrative information and addresses Csquare preparedness and readiness.

- **Business Resiliency Standard** guides the comprehensive business continuity, emergency action, and disaster recovery plans aligned from individual data centers to our corporate headquarters. This top-down methodology requires collaboration from site-level personnel to produce a strong emergency response procedure that is applied consistently to support every data center.
- **Business continuity** is codified in our business resiliency standard – we determine which IT assets and systems are critical, so there is no interruption to customer environments. We achieve this by

conducting a business impact analysis that accounts for business interruption, critical systems, and examination of redundancies. This determines which steps must be taken to prevent external factors from impacting Csquare's ability to operate for our clients and stakeholders. Annually, personnel at every data center receive guidance from headquarters to update existing business continuity plans to enable a strong network of transparency that provides rapid aid from headquarters to operational sites during an incident.

- **Emergency Action Plans** focus on the safety of Csquare's personnel and non-IT assets during an emergency, and table-top exercises to test Csquare's response to probable disasters.
- **Risk Assessments** are conducted for each Csquare site. Csquare examines potential environmental disasters and emergencies and conducts a risk assessment that includes an analysis of incident occurrence, adverse impact, and compensating controls in place. Objectives of this analysis include safeguarding Csquare 's ability to mitigate, respond successfully, and restore critical functions required to deliver customer services.
- **Incident Management -** Although Csquare has designed its infrastructure to adjust to disruptions of various severity, adverse events can occur at any time. Upon receiving information indicating an elevated threat or actual incident, the Business Continuity and Disaster Recovery Team immediately assesses the severity and impact to Csquare operations. Incident detection, reporting, and mitigation are key elements of the BCDR Plan.
- **Operations -** Csquare maintains diverse architecture to create redundancies and divergent pathways for power and other critical systems that include network and support operations. In the event of disruption, this ensures our facilities can remain resilient and recover as quickly and safely as possible. Our Customer Care team is available and trained on support protocol to enable assistance to any Csquare customer. Further, the Customer Portal can be managed from any internet connection.

Readiness requires regular updates to information and processes, and the execution of exercises that prepare all personnel to respond to critical incidents. Csquare's Business Continuity and Disaster Recovery Team is dedicated to meeting compliance requirements from auditing agencies and safeguarding site level personnel and assets from the risks of real-world disaster events. While no infrastructure is impermeable to disruption, Csquare takes care to protect its processes, systems, operations, and personnel.

7.1 Infrastructure Maintenance

Integral to our BCDR Plan is the development of facilities and infrastructure to maintain operation during adverse conditions. Our systems are regularly tested and validated through third-party audits.

Csquare has a change management process for all network and facilities maintenance. The change management process includes a process for reviewing completeness (risk assessment, completed test procedure as applicable, metrics for measuring progress, validation, back out procedure, etc.) and accuracy prior to scheduling and implementation.

Csquare strives to prevent disruptions in service and aims to perform maintenance during low traffic times to minimize potential interruptions to customer operations. "Maintenance" time can be classified as either "Scheduled maintenance" or "Urgent maintenance."

- **"Scheduled maintenance"** includes preventive maintenance, repair or updating activities to help ensure the efficient operation of Csquare facilities and infrastructure.
    - Work is performed during a maintenance window established by Csquare or agreed to by Csquare and the customer.
    - 14-day advance customer notification should be given for any work involving a potential loss of system redundancy.
    - 7-day advance notice for network latency.

- **“Urgent maintenance”** is unscheduled maintenance, potentially impacting the customer, requiring rapid remediation to maintain the operation of Csquare facilities and infrastructure.
    - When possible, customers will be notified prior to the urgent work, if there is an anticipated impact to the customer or if the infrastructure resiliency will be reduced to an N condition.

TARGET WINDOW	WORK ALLOWED
Monday – Friday 5PM to 8AM (local time)	• Scheduled maintenance activity that is expected to impact customers • Scheduled maintenance activity that could put infrastructure below N+1 • Any urgent maintenance
Monday – Friday Anytime (local time)	• Maintenance that is not expected to impact a customer • Any urgent maintenance
Saturday – Sunday Anytime (local time)	• Any urgent maintenance • Non-critical and critical system scheduled maintenance

Note: Csquare cannot guarantee maintenance occurs during non-business hours as we have a global customer base.