# Customer Access and Use Policy

**Details of our access policy are in your MSA contract. This policy document only notes select key parts and is not comprehensive. Some facilities have additional requirements or restrictions. This policy is revised and distributed annually.**

## Definitions

**FLDC** = FirstLight Data Center.
**Security Services (FSS)** = Team responsible for security & access of FirstLight facilities.
**Customer Access Administrator (CAA)** = pre-designated customer employee responsible for vetting customer employees or other customer agents for FirstLight Data Center access.

## Security

The FirstLight Data Center maintains 24x7x365 secured facilities with alarms, closed-circuit video, dual authentication access control, multiple logging, and other systems.

**FirstLight requires that all FirstLight Data Center users fully comply with FirstLight security policy and procedures. Customers shall cooperate in maintaining the security of the FLDC by restricting access to authorized personnel.** As SOC, HIPAA, and PCI compliant facilities, FirstLight expects customers to report any potential concerns to a member of Security Services as soon as possible by email physical_security@firstLight.net or by phone 833-656-3232 Option 2

## Access Categories

**Customers:** are defined as non-FirstLight employees that have equipment or services in a FLDC facility. Access is granted to a specific facility. A Customer in one facility may be a Visitor in a different facility. Carrier technicians with access to a FLDC facility are Customers for this policy.

**Contractors (Vendors):** are pre-approved and vetted contractors that provide goods or services for a specific FLDC. The badge they are issued determines the areas they may access unescorted. If the badge they are issued does not allow entry into a specific space, they may only enter other spaces if escorted by a FirstLight representative.

**Visitors (Guests):** are defined as persons accessing a FLDC facility upon advance invitation of an Employee or Customer or Contractor and are not in one of the above categories for the facility they are visiting.

Any individual attempting to gain access to the FLDC that does not have a Customer Access Request Form on file with FirstLight, will be denied entry into the facility. If the circumstances warrant, the person may be allowed access to the initial entry area of a facility, if it exists, until communication with the CAA is established and documented.

# Customer Access and Use Policy

## Access Requirements

- In most cases physical access into a FLDC is allowed 24 hours a day and 7 days a week.
- Any person accessing a FirstLight Data Center must have a FLDC Access Request Form on file in advance of access. This form can be requested via email from Security Services physical_security@firstlight.net
- The completed FLDC Customer Access Request Form is kept on file and may also be stored in other systems.
- All customers and their employees, technicians, agents, contractors, vendors, and affiliates must be individually specified to gain access into the FLDC.
- Each Customer must designate at least one Customer Access Administrator who will be responsible for all documentation of access requests.
- Changes to Customer Access can only be made by the CAA and only with the appropriate form.
- Access Request Forms and special requests will ONLY be accepted by email from the CAA. Email forwards are not accepted.
- FirstLight Customers and Contractors shall be issued a FLDC identification badge for verification of access and activation of selected access control devices. These may be issued in advance or on site depending upon the specific FLDC.
- All persons in a FirstLight Data Center must always display their FirstLight access badge while on FLDC property or within a FLDC building. The badge must always be clearly visible above the waist. If asked, a FLDC user must give their name and the name of the FirstLight customer for which they have been granted access.
- An access card may be only used by the individual to whom it has been issued. Abuse or misuse of access cards may result in removal of the entrant from the building and denial of future access.
- Tailgating or piggybacking is not permitted. Each person with a badge must swipe at each access control device.
- If a customer requires third-party support, the Customer Access Administrator may grant the third-party temporary access. The request must come from or be explicitly approved by the CAA.
- If a customer requires assistance from the data center staff, especially outside of standard business hours, that request must be made 24 hours in advance, if possible, to FLDC@firstlight.net.
- Customers are required to verify their authorized access personnel list on at least an annual basis. FirstLight must periodically audit these lists for certain compliance requirements.
- Customers wishing to schedule a tour should contact their Account Manager to make arrangements at least 1 week in advance of the proposed tour date. All customer sponsored visitors will be required to the follow the standard security procedures for the FLDC, including presenting photo identification.

## Visitor Policy

Customers may bring occasional visitors the Data Center. The person issuing the invitation is responsible for:

1) Obtaining prior approval from the CAA.
2) Escorting the visitor for the duration of their visit.
3) Ensuring their visitor abides by FirstLight policies and procedures.

# Customer Access and Use Policy

A Customer may request escort of a visitor by FirstLight personnel if the request is made at least 4 hours in advance and is accepted by the Data Center personnel. Escorted access time is billable.

## Temporary Access Requests

Temporary access requests should be sent to physical_security@firstlight.net. The request must indicate all the following:

- Customer Name:
- Customer Account Number
- FLDC Data Center Address:
- Visitors Name:
- Contact Phone:
- Date of Visit:
- Estimated Time of Arrival:
- Access Type: **Full Access; Customer escorted;** ← please select one and delete the others.
- Visit Duration (best estimate):

## General Rules of Use

- While moving through a facility, no person may block or attempt to shield his or her face from the FirstLight security systems.
- Doors within the Data Centers are secured and may not be propped open. Doors that are propped open for more than 4 minutes will generate an alert and, in some facilities, will trip the alarm.
- FirstLight reserves the right to access the customer space at any time for any reason, including and without limitation, to perform maintenance and repairs, inspect equipment, measure power draw and temperature and to perform any contracted colocation services.
- Customer space must be maintained in an orderly manner in good repair and condition and must be kept free of litter, cartons, packing material and packaging related items.
- Customers and affiliates are not allowed to eat, drink or smoke within the FLDC except in areas specifically designated by FirstLight, if any.
- FirstLight does not allow packing materials, cardboard, food or drinks in any controlled environment room.
- Customers and affiliates are not permitted to bring any alcohol, drugs or weapons, including guns, knives and mace within the boundaries of the FirstLight Data Center.
- Customer shall insure that their space follows all Occupational Safety and Health Administration (OSHA) Standards. Customer will be responsible for all damage caused by failure to comply with these standards within the customer space and under the customer's control.
- No customer or affiliate may photograph or film any areas of the FLDC unless specifically approved and accompanied by Data Centers Operation.
- No reporters or media outlets are permitted in FirstLight facilities unless they are a collocation customer.
- No FLDC user or any of its agents or affiliates shall touch, access, tamper or interfere with equipment not specifically owned and operated by the user.
- All users must behave in a courteous and professional manner while in the FirstLight Data Center. FirstLight reserves the right to refuse entry or request customers or agents of the customers to leave if they are unable to behave in a courteous and professional manner.

- Contact a member of the DC team for general questions or for facility specific issues while on site or use the Contact information at the end of this policy.

## Equipment Installation

- No equipment may be placed directly onto the floor. Minimum installation height is four (4) inches off the floor using either rack rails or shelves.
- Customers must install equipment so that cooling air is drawn from the cold aisle and equipment exhaust is discharged into the hot aisle. Equipment with non-standard airflow must be configured or installed in a manner that maintains the facility's intended hot-aisle/cold-aisle airflow pattern.
- Nothing may be mounted or installed or stored that has the potential to restrict airflow through the rack.
- Customers utilizing redundant A/B power are recommended to distribute equipment loads across power paths and individual PDU circuits so that either path can support the full connected equipment load following the loss of the alternate path. Customers are responsible for monitoring and maintaining their equipment and PDU loads within rated capacity under both normal and failover conditions.
- Where dual power feeds are available, FirstLight recommends customer equipment have dual power supplies or that single corded devices be powered by an ATS that is dual powered.
- Customer maintains sole responsibility for any connections, wiring, power cables inside the customer space between the demarcation equipment and customer's equipment.
- Customer shall not permit any wiring, cables or equipment connections to enter any other space outside of the customer's defined cabinet, rack or space.
- When and where available, common work areas may be utilized on a first come, first served basis. All shared work areas must be vacated daily, and customers may not leave any equipment in the work area without a customer technician present.

## Equipment Delivery

FirstLight will accept delivery of customer equipment, including third party deliveries, for select Data Centers. A request to accept delivery must be sent to physical_security@firstlight.net in advance.
The request must indicate:

- FirstLight Data Center address
- Carrier
- Number of packages
- Tracking number
- Estimated date of arrival
- Customer contact information (name, phone & email)

## Customer Access and Use Policy

The request must be explicitly accepted by the Data Center.

Deliveries that require a hand truck, pallet jack or a loading dock can only be accepted on traditional business days from 9am to 3pm. Packages that cannot be hand carried into the facility require at least 2 business days' notice.

All deliveries, including third-party deliveries, must clearly indicate the customer name on the outside of the packaging and either a FirstLight Service Order number or a FirstLight Support Ticket number. FirstLight will not accept any shipment that requires payment. Upon receipt, FirstLight staff will:

- Conduct a visual inspection of the external packaging for any damage.
- Verify that the shipped box count matches the shipping receipt.
- Notify the customer of the receipt of the shipment.
- Store packages in a secure area. In the event of damaged external packaging, FirstLight will accept the delivery but indicate the damage, requesting the delivery driver countersign on the shipping receipt. Except for notifying of visible exterior damage, FirstLight will not take responsibility for determining the condition of a damaged delivery.

Any delivery that does not meet all the above criteria may be refused.

## Storage

Prior to the initial installation, customer equipment can be stored in a secure storage room if there is enough space to accommodate the equipment. The availability of the secured storage space is at the sole discretion of FirstLight. Once the initial customer installation is complete, no spare equipment may be stored in any part of a FLDC. Please contact physical_security@firstlight.net in advance to make storage arrangements.

## Contacts

**FirstLight Data Center** - FLDC@firstlight.net
**FirstLight Security Services** – physical_security@firstlight.net
**Urgent Communications** should be made via phone: 833-484-0404 option 2, 2

FirstLight Data Centers

# Customer Access and Use Policy – Addendum – Biometrics

**This facility utilizes biometric fingerprint scanners as part of its access control. Upon their first visit customers will be enrolled in the biometric system. Please allow extra time for that process.**

## Questions regarding biometrics

**Is the use of this system mandatory or could customer employees gain access to the FirstLight facility without providing biometric information? Does another option exist?** All customer facing facilities are secured with biometric 2-factor authorization. If a potential user does not want to provide biometric data, please contact physical_security@firstlight.net for your options.

**How will this information be used?** Exclusively for 2-factor authorization for building access.

**How is this information secured and where will it be stored?** Fingerprints algorithms are stored on a secure server on our internal security network. Access is strictly controlled, restricted to the FirstLight Security Services Department.

**How long will the information be retained?** We retain this information until you leave as a customer, remove the individual from your access list, or we are requested to remove it.

**Who owns the information collected?** While FirstLight stores the data, and we manage the system that uses it for facility access, our end users own their fingerprint data.

**Will this information be shared with any other entity?** No, in addition the system is not accessible from outside our network, by any third party, or by any FirstLight employee that is not part the Security Services Department.

**What meta data is being stored with the biometric information?** Username and access level.