Carrier-1 – Appropriate Use Policy

This Appropriate Use Policy ("AUP") specifies the guidelines for a Customer's use of Carrier-1's services and is binding on all customers that enter into, or subject to, service agreements with Carrier-1. Carrier-1 reserves the right to modify the AUP at any time, with such modification effective upon posting of the modified AUP to this web site. Customers are responsible for ensuring that their users, representatives, agents, or customers comply with the provisions of this AUP. This AUP does not create an express or implied obligation of Carrier-1 to any third party, including without limitation any obligation to monitor or review any data or content on Carrier-1's network or situated in any of its facilities. Any capitalized term not defined herein shall have the same meaning as defined Carrier-1's standard Master Service Agreement (as amended from time to time).

Please direct all questions regarding this AUP to support@Carrier-1.com

Physical Security

Customers may not rekey or tamper in anyway with cabinet or cage locking systems. Prior written consent is required to make any modifications or additions to physical cabinet structures. If Carrier-1 does authorize changes or modifications to cabinet or cage security, Carrier-1 must be provided uninhibited access to the cab or cage. i.e. keys, FOBS, and/or any other means of mechanical and electronic access.

Installation of cameras within the data center, including inside a Customer's cabinet, is strictly prohibited without prior written consent. If written consent is granted, cameras may only capture areas controlled by the Customer and may not face outward or bring into view any other area of the data center. Carrier-1 reserves the right to review footage of customer installed cameras at any time.

Installation or operating of Customer owned Wi-Fi enabled broadcasting network equipment is strictly prohibited within the Data Center without prior written consent. Carrier-1 reserves the right to immediately power down and remove any device deemed to have Wi-Fi capabilities within the Data Center.

Installation of Customer owned Uninterruptable Power Sources (UPS) within a Customer's cabinet is strictly prohibited. If a UPS is discovered to be in use within a Customer's cabinet Carrier-1 reserves the right to immediately power down the cabinet and remove the UPS without prior notification to the Customer.

Adjusting, tampering, removing or otherwise altering power distribution units (PDU) supplied by Carrier-1 or Customer that void the UL certification of the product is strictly prohibited. If it is deemed by a Carrier-1 employee that a PDU has been altered in any way that it affects the UL certification of the product, Carrier-1 reserves the right to immediately power down the cabinet and remove the PDU.

All electrical devices and connections must meet NFPA, NEC, and local city electrical code. Devices and connections that do not meet with these minimum requirements, are subject to immediate electrical isolation until corrections have been completed.

If any of the above events requires Carrier-1 to dispatch an engineer or facility team member, Carrier-1 reserves the right to charge customer $250/hr.

Illegal Data and Content

Customers shall not store or transmit data or content that Carrier-1 determines, in its sole discretion, to be in violation of any applicable law, regulation, or order of a court of competent jurisdiction. Carrier-1 reserves the right to cooperate fully with any law enforcement authorities regarding any such data or content. Customers shall be responsible for determining what laws or regulations are applicable to their use of the Services.

Abusive Network Activities

Customers may not engage in, or allow, any activities that Carrier-1 determines to be abusive network activities directed towards any third party or Carrier-1, which include, without limitation, the following:

- Forging of message headers or sender identity information
- Introduction or propagation of malicious programs (e.g., Trojan Horses, Internet viruses, worms, key loggers)
- Engaging in the unauthorized circumvention of the security or authentication procedures of any host, application, account, or network
- Executing any interference or denial of service to any host, application, user, account, or network
- Intercepting any Internet data not destined for Customer's host server
- Disrupting network activity, such as by ping flooding, forged router information, port scanning, email-bombing, packet spoofing, IP address spoofing.

Customer Security Responsibilities

Customers are solely responsible for any breaches of the security of any servers or networked hardware under its control or ownership, including safeguarding all authentication and account information. Carrier-1 may immediately, and without prior notice or service credit, disconnect any Customer server that it suspects to be involved in any illegal or abusive network activity and initiate an investigation to determine the cause of such activity. Customers are responsible for all costs and expenses incurred by Carrier-1 and any third party who was damaged by such illegal or abusive network activity. Customers must immediately notify Carrier-1 of any illegal or abusive network activity by contacting Carrier-1 at abuse@Carrier-1.com

Intellectual Property Infringement

Customers may not store or transmit any data or content that infringes on a third party's intellectual property rights. Carrier-1 may remove or disable access to any allegedly infringing data or content in order to comply with any court order, regulation or law. CARRIER-1 MAY PERMANENTLY SUSPEND OR TERMINATE SERVICES TO ANY CUSTOMER THAT ENGAGES IN REPEATED VIOLATIONS OF THIS INTELLECTUAL PROPERTY INFRINGEMENT POLICY OR ANY APPLICABLE LAW.

Prohibited E-mailing Activities

Customers may not send, or allow to be sent, unsolicited emails ("Spam") over Carrier-1's network. Customer may send e-mail only to parties who have expressly requested to receive such e-mail via a "double opt-in" confirmation process. Customers must maintain complete and updated records of all opt-in consents (including the e- mails and headers from each consenting party) and immediately provide such records and sufficient proof of all consents to Carrier-1 upon request. The aforementioned policy applies to Customer-operated list servers, mail lists, or mailing services that do not target an audience that has expressly consented to receiving such e-mail.

Customers may not engage in the following e-mailing practices:

- E-mail header spoofing or forgery
- Use of the Services to receive replies to Spam
- Host web pages that are advertised in Spam sent from another network
- Using third-party proxies in any way to cause the transmission of Spam

Carrier-1 reserves the right charge Customer $250 per hour in consulting fees for any remedial actions that Carrier-1 elects to take in the event that, as a result of Customer's activities, Carrier-1's servers or IP space are placed in any third-party mail filtering software or black hole lists.

Cooperation with Investigations

Carrier-1 may engage in any reasonable action, without prior notice to Customer, relating to the Services in order to comply or cooperate with any civil or criminal investigation or cause of action regarding Customer data located on Carrier-1's network or Customer-owned equipment located in Carrier-1's facilities.
Carrier-1 shall not be deemed to be in breach of any service agreement, nor will it be obligated to grant any service level credits, for any disruptions to the Services.

AUP Enforcement

Carrier-1 reserves the right at all times to take any necessary actions to enforce this AUP, including suspending, terminating, or limiting the scope of the Services to a Customer, and shall not be obligated to issue any service level credits or other compensation for any resulting interruption in Services. Customers are responsible for any expenses that Carrier-1 incurs for enforcement and remedial measures in connection with AUP violations, including the payment to Carrier-1 of emergency- rate consulting fees.

Last modified: May 9, 2016