



Acceptable Use Policy

This Acceptable Use Policy specifies the actions prohibited or restricted by Switch Communications Group, L.L.C. ("Switch") to users of the Switch Internet Network and the Switch Colocation Facilities (collectively, the "Facility"). Switch reserves the right to modify this Policy at any time, effective upon posting of the modified Policy to the following URL: http://www.switchnap.com/media/switch_aup_agreement.pdf

Illegal Use

Customer's use of the Facility must be in strict conformance with all applicable laws and regulation and to the terms of the Customer's Agreement with Switch.

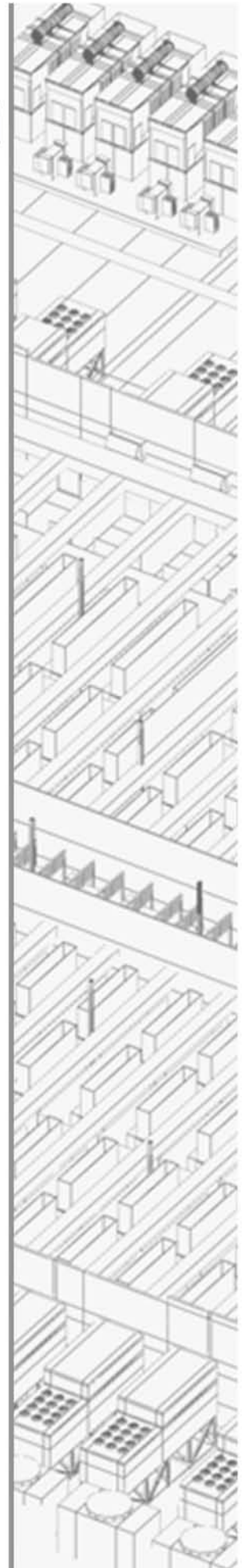
Facility Power

Each Switch Facility is designed to meet Uptime Institute's Tier 4 standards for power throughputs. Mission critical power for a Facility is built out as needed and there may be periods of time that require extended installation timeframes. Once mission-critical power is fully consumed at a Facility, no more power will be available at that Facility. Power circuits are made available on a first-come, first-served basis, and all service orders must be in writing, signed and dated to reserve power. All power circuits ordered will be at the then posted retail rates for the date that the service order is signed and are subject to change. Per National Electric Code, current delivery cannot exceed 80% of a circuit breaker's rated capacity. If a Customer consumes electrical power above the 80% breaker capacity, the Customer will be billed a special allocation fee of \$1,000 per offending cabinet per month until the usage is corrected. If the Customer requires power in excess of Tier 4 thresholds then the Customer shall comply with Switch's request to move the Customer to Switch's higher density power Facility at no cost to Switch. All power circuits must be utilized solely to power the cabinet to which the circuits are assigned.

Customer UPS's are not allowed to be used down-line from the Switch mission critical power system. Switch Operations must approve all power distribution systems prior to deployment within the Customer's collocation space. All Customer equipment must first be tested on house power prior to plugging into the Switch UPS receptacles.

Heat Containment

The delivery of high-density power is only possible if the exhausted equipment heat is contained and prevented from mixing with the cold air in the Facility. Switch has created the Thermal Separate Compartment in Facility (t-scif™), a state-of-the-art, patented system which offers Customers the luxury of high-density power in a safe environment. Customers collocated in a t-scif™ must comply with the standards and procedures required to make this environment successful for everyone. All equipment must vent heat into the center hot aisle, either directly or via custom directional airflow devices. The doors to the hot aisles must remain closed at all times unless entering or exiting the hot aisle and the doors must never be propped open. Blanking plates must be used to close off any open sections of customer cabinets. Customer agrees to minimize Customer's





Heat Containment Continued...

carbon footprint by working with Switch to maintain a hot aisle temperature between 100° and 110°. All Customer Equipment must be UL60950 compliant or other standard acceptable to Switch. The Customer Equipment and its installation must conform to the requirements contemplated by ANSI / NFPA 70. Customer shall not install equipment that requires the additional safeguards contemplated by ANSI / NFPA 70, Article 645 and NFPA 75. Refusal to cooperate with these standards will be treated as a direct violation of this Acceptable Use Policy.

System and Network Security

Violations of system or network security are prohibited, and may result in criminal and civil liability. Switch will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected.

Examples of system or network security violations include, without limitation, the following:

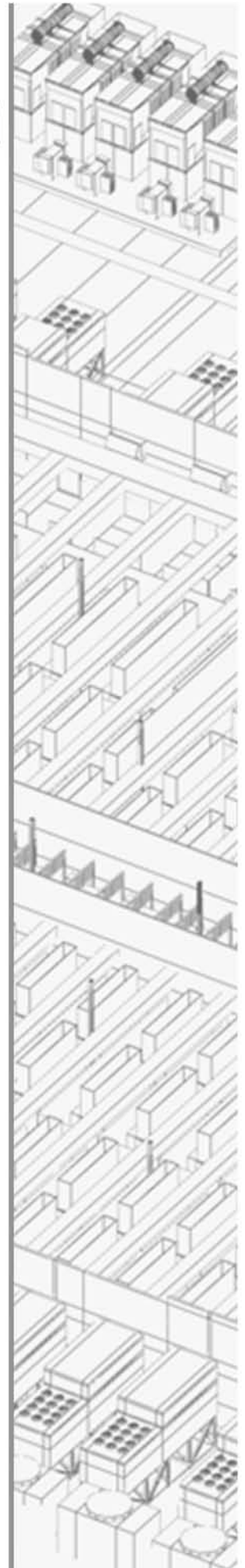
- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting

Network Integrity

It is strictly prohibited to take or cause another to take any action which (i) provides access to the Switch Network from outside of a Switch Facility; (ii) extends the Switch Network beyond the Switch Facility in which access is initially provided by Switch; (iii) is in violation or which would cause a violation of Switch's competitive data center carrier interconnections; (iv) resell, pass-through, sublicense, rent, lease, timeshare or rebrand the Switch Network or Switch's services or otherwise provide access to the Switch Network to any party not within Customer's enterprise, or (v) in any way provides a non-Switch customer with access to the Switch Network other than a permitted third party physically located within the Customer's colocation space. Switch reserves the right to grant limited exceptions to the foregoing restrictions to accommodate unique circumstances.

Cross-Connects

Carriers and resellers who do not have a signed, current Carrier Access Agreement in place with Switch may be denied cross-connects. Carriers who have not signed a Carrier Access Agreement are prohibited from utilizing any approved carrier to access any Switch facilities. Switch reserves the right to remove any unauthorized cross-connects or connections that could compete with Switch's business interests or violate the client connectivity terms of the Switch AUP with or without prior notification.





Cross Connects Continued...

Cross-connects between connectivity providers that are intended to use Switch facilities as a pass through to connect to other non-Switch-owned data centers within a 50 mile radius to the Switch facilities are not allowed without Switch's explicit, written permission. Cross-connects to third party facilities are priced at \$500.00 per month.

Email

Sending unsolicited mail messages, including, without limitation, commercial advertising and informational announcements, is expressly prohibited. A Customer shall not use a third party's mail server to relay mail without the express permission of such third party.

Connectivity Pathways

Any and all telecommunication connections, whether dark or lit, which access internal or external telecommunication vaults, easements, rooftops and/or connectivity paths located on any Switch property that utilize (or could utilize) a Switch facility as a pass through to connect to other non-Switch-owned multi-client data centers within a 50 mile radius to the Switch facilities are not allowed without Switch's explicit prior written permission, which may be granted or withheld in Switch's sole discretion.

Usenet

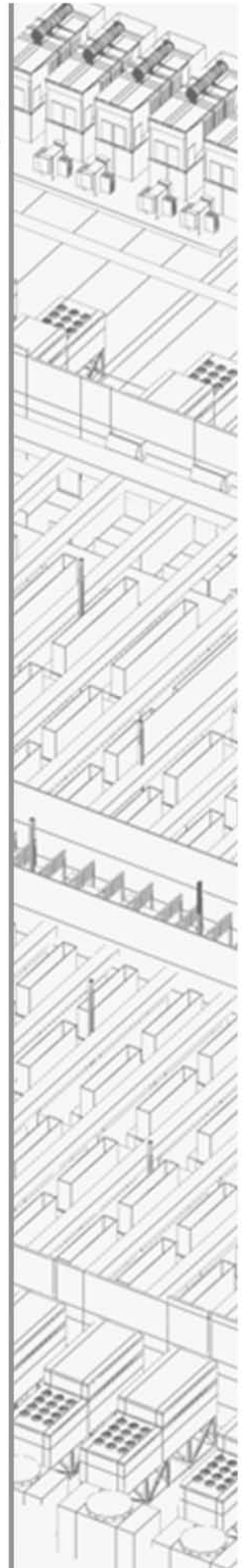
Posting the same or similar message to one or more newsgroups (excessive cross-posting or multiple-posting, also known as "SPAM") is expressly prohibited.

Conduct / Third Party Entry

All individuals entering the datacenter must conduct themselves in a professional manner at all times both in keeping with their particular industry and generally applicable standards of courtesy. Only qualified professional laborers are allowed to perform work onsite. All clothing must be professional and provide adequate coverage and protection. Close toed shoes are highly recommended. Open toed sandals are not permitted. Sleeping is not permitted in the Facility including on the datacenter floor. Proper grooming and cleanliness are required.

Due to the secure nature of the Facility, Customers may not bring third parties to the facility to provide a tour of the Facility or for any reason other than vendors providing services to Customer's colocation space. This includes members of the media. All tours must be conducted by Switch personnel. Video, photography and audio recordings are strictly prohibited within the datacenter.

Customer must adhere to industry standards for cable management. Cables must be properly installed and either enclosed in cable management trays or in clean bundles for proper presentation and identification. Switch will not provide Smarthands services to cabinets with improper cable installation or management.





INDIRECT OR ATTEMPTED VIOLATIONS OF THIS ACCEPTABLE USE POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A SWITCH CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER AND MAY RESULT IN SUSPENSION OR TERMINATION OF ACCESS TO THE SWITCH NETWORK (INCLUDING THE DISABLING OF CROSS-CONNECTIONS) AT SWITCH'S SOLE ELECTION.

Complaints regarding illegal use or system or network security issues may be sent to

abuse@switchnap.com.

Complaints regarding SPAM or other email abuse may be sent to

abuse@switchnap.com.

Complaints regarding USENET abuse may be sent to

abuse@switchnap.com.

For live security incidents, please contact

Switch Internet Abuse Investigations

at

1-866-262-0895

(24x7)

