

DataSite - Orlando
Data Center Policies
&
Work Rules



DATA **SITE**
ORLANDO

DataSite Data Center Policies & Work Rules

The following policies regulate activities at the DataSite Data Centers (Data Center). These rules are intended to ensure the safety and security of individuals and equipment at the Data Center. Failure to adhere to these rules may result in the expulsion of individuals from the Data Center and could result in the declaration of default by DataSite for the Customer and the termination of the Customer contract. Appropriate response to violations of these rules shall be solely within the discretion of DataSite. DataSite reserves the right to update, modify or amend these rules, as necessary.

A. General Guidelines

1. All Customers and Customer vendors shall conduct themselves in a courteous professional manner while visiting the Data Center. Customers shall refrain from using any profanity or offensive language.
2. Customers may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
3. DataSite is not responsible for any loss, damage or theft of vehicle or the contents thereof, while located in a Data Center parking area.
4. Alcohol, controlled substances, firearms and explosives are not permitted on DataSite property. Smoking, drinking, and eating are strictly prohibited within the Data Center raised floor space. Smoking is expressly prohibited in all DataSite buildings.
5. Persons under 18 years of age or requiring adult supervision are not permitted within the Data Center without the express written permission of DataSite.
6. All visitors to the Data Center should wear appropriate footwear and attire.
7. Unless otherwise expressly permitted by DataSite in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center. Customers are expected to be familiar with and adhere to all OSHA standards associated with work in a computer room environment
8. Customers may use cell phones inside the Data Center. Two-way radios are not permitted the Data Center. Cell phones with camera capabilities may not be used for picture or video capture.
9. Skateboards, skates, scooters, bicycles or other types of vehicles are prohibited in the Data Center.
10. Sharing DataSite Proprietary information, without the express written permission of DataSite, is strictly prohibited.
11. All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center are subject to inspection by Data Center staff and/or Security.
12. DataSite does not accept Mail/Post on behalf of Customers at the Data Center. All Mail/Post should be directed to customer's business address.

13. Customers must cooperate and obey all reasonable requests of Data Center personnel while within the Data Center, including immediately addressing any violations of rules when brought to Customer's attention.
14. Upon activation of a smoke detector or emergency alarm, all Customers (their employees and vendors) must be prepared to evacuate the building and to receive further instructions from the DataSite staff.

B. Pictures or Video

15. Any use of cameras, video and other photographic equipment along with but not limited to audio monitoring and audio capture devices are prohibited within the Data Center without the express written permission of DataSite. No person, other than Data Center personnel, shall be permitted to take photo or videotape records within the Data Center.
16. Customers are not permitted to take pictures or videos of the Data Center. Customer site pictures or videos must be arranged in advance and according to DataSite Security regulations.
17. If pictures or video are required for insurance or marketing purposes, contact DataSite assistance.
18. All types of cameras, unless otherwise provided in this Service Guide, are prohibited in the Data Center.

C. Physical Security

19. DataSite Data Centers are secured facilities. Access to the data center and other areas of the facility are restricted to those persons with authorization.
20. Customers are restricted to authorized areas only, including the lobby, customer lounge, conference rooms, common areas and customer space on the data center floor.
21. Security controls include 24 x 7 security officer presence, sign-in procedures for all ingress and egress, managed key and access card plans, man trap, managed access permissions and access request methods.
22. Closed-circuit television (CCTV) cameras are used to monitor all areas of the facility including lobbies, common areas, customer lounge, data center floor space, admin areas, and engineering plant areas for your safety. All CCTV cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.
23. DataSite attempts to provide off street parking, where feasible, with adequate lighting. DataSite is not liable for damage, loss, or theft of vehicles and/or contents
24. Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited.
25. Exterior Data Center doors may not be propped open. These access doors are monitored and alarmed.
26. DataSite reserves the right to access any part of the Data Center at any time for safety and security reasons.

D. Data Center Ingress and Egress

27. All persons entering the Data Center must:
 - a. Possess a valid government issued photo ID.
 - b. Have authorization to access the facility.
 - c. Sign-in and out as required by the facility.
 - d. Display their DataSite security badge at all times while in the facility.
 - e. Surrender their security badge, access cards, keys, DataSite owned tools or phones prior to exiting the facility.
28. Customers are expected to be familiar with and adhere to all OSHA standards associated with work in a computer room environment.

E. Access List Management

29. Customers are responsible for maintaining and updating their access list. DataSite requires a written submission for additions and deletions to the Customer's access permissions list. Individuals identified on this list will be granted access to the Customer's Cabinet, Cage or Suite. Customers may grant temporary access to their Cabinet, Cage or Suite for an employee, vendor or technician by submitting an Access Ticket to clientsupport@datasiteorlando.com (see Exhibit I).
30. DataSite is not responsible for providing access to or for the activities of individuals whose authorization is reflected in Customer's access list which was not updated by Customer to revoke such authorization at the time such access was granted by DataSite. The Customer remains responsible for the activities of these individuals as with any other authorized Customer employees, contractors or vendors.

F. Common Areas and Customer Lounge

31. The common areas, Customer lounge, and conference room areas within the Data Center are for the common use by all DataSite Customers with sites within their respective Data Centers.
32. The Customer lounge and associated Internet access is provided as a courtesy to Customers. Customers shall use such Internet access for business purposes only and follows DataSite acceptable use policy.
33. The Data Center common areas are offered as a convenience and not as a work area. Extended use or monopolizing all or some of the working assets of a Data Center Common Area, as listed above, for more than 2 hours (total) in a 24-hour period is not permitted in the Data Center common areas.
34. Customers using the common areas must throw away their trash in the appropriate receptacles. If you reserve and use a conference room, please be responsible for clean up after using the facilities. Coordinate all catering events through the management of DataSite.
35. Customers may request dedicated administration space or reserve a conference room by submitting an email to operations@datasiteorlando.com .

36. A staging area is available, on a first-come, first-served basis, for the temporary unpacking and configuration of servers. The staging areas are offered as a convenience and not as a permanent storage area. Extended use or monopolizing all or some of the staging areas of a Data Center, as listed above, for more than 14 calendar days in any 30-day period is not permitted in the Data Center staging area. Equipment assembly and similar functions are restricted to the staging area may not be conducted in common areas. DataSite is not liable for Customer assets left unattended in this area. If you wish to lease a staging cage for regular (non-temporary) basis, please contact DataSite.
37. DataSite reserves the right to deny access to those Customers who abuse the common areas and the rights of other Customers.

G. Cage/Cabinet and Cabling Requirements

38. Customer cage or cabinet shall, at all times, be clean, neat and orderly. Customer space shall not pose any danger or hazard to customer or employees (including subcontractors) that may be requested or required to enter the cage to perform a service or to any other customers of the Data Center.
39. Customers must take all necessary precautions to ensure the physical security of property contained within their customer location(s). Cage and cabinet doors must be secured at all times when a Customer is not physically present.
40. Customers must remove all refuse materials (which include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of Customers' equipment) in the Customer Area from the Customer and Common Areas within eight (8) hours. Materials must be placed in designated disposal
41. The creation of "office space" within the Customer Area on the Data Center Floor is prohibited.
42. All spare equipment shall be stored in a cabinet or must be kept in approved plastic or metal containers. Containers must be sealed, stacked neatly and can not impede ingress/egress or cooling.
43. "Un-racked", operating equipment outside of cabinets or racks, is strictly prohibited.
44. No combustible material, i.e. cardboard, foam, or paper may be stored in Customer cabinet or cage.
45. Remote Hands Service requests may be denied should Customer's Cage, Cabinet or Suite be identified as noncompliant with DataSite Data Center Policies regarding refuse and combustible materials
46. Customer may not hang or mount anything on the cage mesh walls or cabinets unless authorized by the Data Center Management staff.
47. The tops of the cabinets or ladder rack may not be used for physical storage.
48. To ensure maximum ventilation Blanking Panels must be utilized on all open rack spaces within and between racks at all time.

49. Unsecured cabling across aisles or on the floor is strictly prohibited. All devices must be installed in racks or cabinets. Ladder racking must support all cabling between rows.
50. Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet. Should Customer need assistance with cable management, Customer may open a trouble ticket with DataSite
51. Cabling must not obstruct airflow/ventilation/AC (perforated tiles) or access to power strips.
52. Remote Hands Service requests may be denied should Customer's Cage, Cabinet or Suite be identified as noncompliant with Industry Best Practices. Industry Best Practices for cabling standards is the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Cabling Standards 568 and 569.
53. DataSite reserves the right to decline implementation of a Change Order if DataSite determines the Customer cage, cabinet or cabling is not in compliance. Customers in violation will be notified by DataSite in writing and Customer must remedy the situation immediately. SLAs do not apply until the cage, cabinet or cabling complies with the requirements.
54. If Customer intends to use Remote Hands Services, all devices and cabling must be clearly labeled in a unique naming fashion. In order to reduce confusion, there should never be two devices or cables with the same name. DataSite recommends that Customer should not use its name as a naming convention to protect Customer privacy and confidentiality. For additional security purposes, external I.P. addresses should not be visible from outside of the customer's space.
55. Non-compliance with any of the cage, cabinet or cabling requirements will result in notification to Customer and a request that the Customer promptly take action to remedy the situation. Customer failure to remedy the situation will result in assessment of time and material fees if DataSite takes action to make the Customer cage, cabinet or cabling compliant.
56. Customer may not climb onto cabinet and or scale cage walls. Customer must request Data Center Staff assistance when needing to access cabinet / rack tops.
57. Customer may not make physical alternations or modifications to the space, without prior written permission from DataSite.
58. Customer failure to remedy any violation of the DataSite Data Center policies will result in assessment of time and material fees if DataSite takes action to make the Customer Cabinet, Cage or Suite compliant with the policies set forth.

H. Rack/Cabinet Doors

59. Cabinet doors may be removed while Customer is working within the cage and must be replaced before Customer exits the Data Center.
60. If Customer cabinets are equipped with doors, the doors must be closed when Customer is finished working on devices.
61. Should the locks or doors not function properly, Customer should contact the on-site Data Center Management staff for assistance. Do not pry, bend, or force the

doors open. Customer shall be responsible for any repair charges associated with any damage to doors caused by Customer.

62. Cage doors should be closed and locked to prevent unauthorized access.

I. Floor Tiles

63. Customers are prohibited from lifting or moving floor tiles. The sub-floor area is restricted area, accessible by DataSite staff only. The perforated tiles are strategically placed for HVAC cooling patterns. If Customer is experiencing temperature problems, Customer should notify DataSite to open a trouble ticket. Only DataSite staff is permitted to access the sub-floor.

J. Data Center Equipment

64. Data Center equipment such as tools, dollies, carts, server lifts, monitor and keyboards will be available to Customers on a first-come, first-served basis. Customer is responsible for all loaned equipment while it is checked out and shall return the equipment immediately.
65. Modification of equipment on loan from the Data Center is not permitted without prior written approval from Data Center management.

K. Shipping and Receiving

66. Customer may bring small “hand carry” equipment through the lobby. Customer may contact Data Center Staff or Guards for assistance. Large amounts of equipment, shipments or large devices must enter the Data Center through shipping/receiving dock. Customers must notify DataSite management of any such deliveries that will require processing through the loading dock by submitting an email to operations@datasiteorlando.com .
67. Hand carried equipment brought into the Data Centers may require DataSite technician assistance with the installation to help calculate the additional power draw of any new equipment being added to a customer’s rack. This assistance is to help ensure customer power SLAs are not jeopardized. To ship equipment, contact Data Site 10 days prior to shipment delivery to alert the Data Center of a delivery.
68. All packages shipped to the Data Center must have the Customer’s name and site ID on the shipping label. Unidentified packages are a security risk. Any unidentified packages delivered to the Data Center will be refused for security reasons. Packages and smaller shipments will be received and stored in the locking cages in the Customer Staging area. Customers will need to coordinate pick-up of such items within a period of time no longer than two weeks.
69. Unless agreed to in writing by DataSite, all equipment received at the Loading Dock must be removed to the Customer Area or other authorized area, within 4 days of its arrival at the Data Center. Customer will be charged storage fees for any equipment remaining in the Loading Dock area more than 4 days.
70. Data Center staff will not move, unpack or uncrate any Customer owned equipment (racks, cabinets, racks of equipment, etc) greater than 300 pounds. Customer is responsible for unpacking, uncrating, and movement of heavy equipment to the Data Center floor, including all associated costs.

71. Customer, in coordination with the Data Center staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure (plywood on raised floors, cage wall removal, overhead clearance, etc). Observe posted signage in the shipping/receiving area that egress points to raised floor areas noting that Customer should “Please contact Data Center staff before moving equipment greater than 300 pounds to the Data Center floor.”
72. The Data Center will not pack and ship any Customer owned equipment. The Customer may open a ticket to authorize temporary access for their shipping company to enter their cage and cabinet, or to have the data center staff de-rack a device and make it available to the Customer’s shipping company.
73. Customer is responsible to ensure their shipper provides all packing material and physically packs the devices for shipping them. DataSite shall not be liable for improper packing and shipping of Customer owned devices.

L. Audits

74. All Customer requests for audits shall be made in writing and submitted to DataSite. All desired audit points must be defined in the request for review. Unauthorized audits are strictly prohibited.

M. Removal of Equipment at End of Term

75. Unless otherwise agreed to in writing, Customer will have all customer-owned hardware removed from the Data Center no later than the Effective Cancellation Date. Customer-owned hardware remaining in the Data Center after the Effective Cancellation Date becomes the property of DataSite.
76. Upon termination or expiration of Service, Customer must leave the Space in as good condition; normal wear and tear excepted, as it was at the Commencement Date, and must remove any Customer Equipment and other Customer property from the Space.
77. Refer to the Service Guide for Cancellation guidance.

N. Web Cams and Audio Monitoring devices

78. Web cams may be permissible as long as they are fixed-mount placements with no pan-tilt-zoom capabilities and the field of view is limited to Customer’s cage floor space ONLY. The camera manufacturer and model number will be submitted through the change order process to be given the opportunity for Data Center Management to conduct an Engineering Review of the camera. Cameras found not to be compliant will not be allowed into the center.
79. The Data Center Management staff must verify the field of view of all cameras. Should the device be moved after verification, DataSite reserves the right to deny the use of the camera until it is in compliance with the limited field of view requirements. Data Center Management will disable any camera found to be non-compliant through physical means, until the camera can be proven to be in compliance.

80. Audio monitoring and audio capture devices are expressly forbidden in the Data Center.

O. Environmental Devices

81. If you install environmental sensing devices in their cage or cabinet, the readings obtained will be considered secondary to Data Site's environmental monitoring.
82. Individual or free-standing electrical devices such as humidifier/dehumidifier, fans, air circulators, or air filters are not permitted in cage areas or cabinets. Fans integrated into racked equipment (servers, routers, switches) and customer provided racks are permitted. Should Customer need assistance with environmental conditions, Customer may open a trouble ticket with DataSite.

P. Customer Provided Racks

83. Customers may provide their own racks or cabinets upon approval in Engineering Review. The dimensions and height of the Customer provided cabinet must be listed in the SOW. DataSite will mount Customer provided racks to ensure proper grounding and compliance with all applicable ordinance codes.
84. If the height or depth is greater than the specified DataSite standard, the rack or cabinet must be reviewed by DataSite for weight, HVAC impact, and CCTV camera field of view impairment.
85. Additional Space may be required if a standalone DataSite locking cabinet exceeds the maximum allowable power as defined in the collocation services agreement or if a Collocation Suite or Custom Data Vault exceeds the maximum allowable watts per square foot of power utilization as defined in the collocation services agreement

Q. Customer Provided Power Strips

86. Use of customer provided power strips must be discussed and reviewed with DataSite account team. Power strips must be UL or industry approved; provide some type of over-current protection; and, must be mounted in the racks. If DataSite determines the receptacles need to be changed to accommodate the Customer provided power strips, additional charges may apply.
87. Customers are prohibited from plugging their own power strips into DataSite or customer provided power strips (daisy-chaining). This is in violation of electrical and safety codes and DataSite reserves the right to demand their removal. Any violations of this policy must be rectified within one business day. Failure to correct this violation after one business day is a material breach of the terms of the customer's contract.
88. Customer provided power strips are considered custom power.
89. DataSite shall not be responsible for an outage caused by a Customer provided power strip.
90. Customer requested power audits must be requested via the remote hands ticket process.
91. DataSite may conduct periodic power audits of Customer Space. Any violation of power limitations must be addressed immediately. Please refer to the Service Guide for additional information.

R. Customer Provided Additional Security Devices

92. Customers are not allowed to add security devices that would hinder Data Site's access to the cage or cabinet. This is for security and safety reasons. DataSite must have access to all areas of the Data Center at all times.

Exhibit I:
Example of an “Access Ticket”

Subject: Customer # 00101 Access Ticket for 12/20/09

Access Ticket:

Customer # 00101 ; ABC Corporation

Name and vendor: **John Doe (IBM Technician)**

Task being performed: **Working on the IBM Storage Array.**

Start Date\Time: **12-20-2009 at 01:00 PM**

End Date\Time: **12-20-2009 at 05:00 PM**

Location of Task: **ABC Corporation’s cage in Data Center**

Escorted or Not Escorted: **Will need to be escorted to cage (not on access list)**

*Bill Smith
Director IT
ABC Corporation*

Any additional comments or info relevant to this person’s access go here.



Exhibit II:

Personal Accountability

Failure to knowingly comply with the following procedures is grounds for immediate removal from the facility. All persons allowed access to critical areas must review these policies and work rules and demonstrate their understanding of these procedures most applicable to their activity.

It is vitally important that you understand the potential for negative impact your actions could have on this site as a result of working inappropriately and our desire to avoid such instances. These procedures and guidelines have been developed to clarify our quality expectations and to reduce the chance of mistakes and unintended events. Failure to comply with any procedure may result in your immediate removal from the site and may result in permanent loss of your access to the facility.

I have been given a copy of the DataSite - Orlando Data Center Policies & Work Rules and acknowledge their receipt. I have had an opportunity to review and ask questions about these procedures and policies. I agree to follow these procedures and policies to the best of my abilities.

Company _____

Name [print] _____

Signature _____ Date _____

Accepted by DataSite _____ Date _____

If at any time you have questions or require assistance use the following numbers:

- General Manager: Office (407) 591-5850 -/- Mobile (407) 488-2941
- Security: (407) 591-5810 -/- 5911