Logista Data Center Use Policies and Regulations

Revision Date: 6/26/2012

This Use Policy and Regulation document, including the following list of Prohibited Activities and Security Procedures, is an integral part of your Colocation Agreement with Logista. If you engage in any of the activities prohibited by this document Logista may suspend or terminate your account. Logista's Data Center Use Policy and Regulations (the "Policy") is designed to help protect Logista, Logista's Data Center, and our customers from irresponsible or illegal activities. The Policy is a non-exclusive list of the actions prohibited by Logista, which reserves the right to modify the Policy at any time.

1. Use of Colocation Facilities, Building and Customer Space

1.1. Customer shall maintain its space in an orderly and clean manner and in good repair and condition, satisfactory to Logista. Customer shall keep the Space free of litter, cartons, packing materials or packaging and related items (collectively "waste materials"). Customer shall deposit all waste materials in designated trash receptacles that may be located in the colocation facility or within or outside of the building. Under no circumstances shall waste materials be discarded or left in the colocation facility, or the building. Customer shall deposit all non-hazardous waste in appropriate receptacles located outside the building. Logista does not provide and is not responsible for providing receptacles for Customer waste materials.

1.2. Customer shall insure that their Space is in compliance with all Federal and State Occupational Safety and Health Organization (OSHA) standards. Customer will be responsible for all damage that may be caused by failure to comply with any OSHA standards within the space and under the customer's control.

1.3. Customer shall not eat, drink, or smoke within the colocation facility or the building, except in areas designated by the building management.

1.4. Customers shall not bring any weapons, including guns, knives or mace, alcohol; or drugs within the colocation facility or the building.

1.5. Logista and RSA reserves all rights to escort any person(s) out of the facility thought to be a danger to the facility, other personnel, or to themselves. Examples include, without limitation, public intoxication or the smell of liquor on their breath or disreputable behaviour.

1.6. Customer shall not photograph, videotape or film any areas in the colocation facility or the entrances to the colocation facility.

1.7. Customer, its officers, employees, technicians, agents, representatives, subcontractors and visitors shall behave in a courteous and professional manner at all times while in the facility.

1.8. Customer, its officers, employees, technicians, agents, representatives, subcontractors and visitors shall not touch, access, tamper, or interfere with another customer's Space or equipment without such customer's written authorization, even if Customer owns equipment within another customer's Space.

1.9. Customer, its officers, employees, technicians, agents, representatives, subcontractors and visitors shall not loiter or solicit within the colocation facility, the building in which the colocation facility is located, or on the grounds that the colocation facility is located.

1.10. Customer shall not do or permit anything to be done, or fail to do or permit anything to be done in, on or about the building that might constitute or result in a private or public nuisance or waste.

1.11. Customer shall not make any alterations, additions or improvements to the Space without the prior written consent of Logista or RSA.

1.12. Customer shall not, nor shall Customer permit others to: (i) fail to maintain a suitable environment as specified by Logista; (ii) alter, tamper with, adjust or repair any equipment or property of Logista or any other property (other than its own equipment inside Customer's Space) located within the colocation facility or the building; or (iii) abuse or fraudulently access the building or the colocation facility to obtain or attempt to obtain service by any means or device with intent to avoid payment, unauthorized access, alteration or destruction, or any attempt thereof, of any information of Logista or any other customer of Logista by means of devise, use of any equipment in violation of the law or in aid of any unlawful act, use any equipment so as to interfere with the use of the telecommunications network operated by Logista or customers or authorized users or in a manner

which, in the opinion of Logista is not in accordance with its generally accepted standards of Telecommunications access and use.

1.13. Customer shall wear slip-resistant shoes while on the Data Center floor and inform Logista technicians immediately of any unsafe facility conditions of which the Customer is aware (e.g., loose ladder racks, slick floors or electrical issues).

1.14. Each Customer cage and cabinet in Logista facilities are designed to provide colocation to an individual customer and Logista does not allow more than one customer per customer cage or customer rack in any Logista facility.

1.15. Customer may not prop open any doors within the facility.

1.16. No one may shield his or her face in any manner from the security system. All Customer employees, vendors and visitors must display their access badge or visitor badge prominently AT ALL TIMES.

2. Power

2.1. Power provided will be based solely on accepted equipment configurations as set forth on the duly executed Logista Colocation Services Agreement. Logista will provide redundant A and B feeds for DC power. RSA may (with 24 hour notice) temporarily remove from service any individual power feed for maintenance of the power infrastructure. Customer may not use a redundant power feed as an individual power feed.

2.2. Customers may not install any batteries in the colocation facility.

2.3. Customer must inform Logista immediately upon discovery of any worn, frayed or cut cables.

2.4. To insure the safety of the Logista facility, each cabinet installed in the Space may have a circuit maximum of 60 Amps AC (7,200 watts) or 60 Amps DC power. Each rack may have a circuit maximum of 100 Amps AC (12,000 watts) or 120 Amps DC power.

2.5. All equipment utilized in the facility must meet Underwriter Laboratory (UL) listing or a similarly recognized governing board.

2.6. Customers may not plug any equipment into receptacles or courtesy power outlets without the express written permission from Logista.

2.7. No equipment specifically designed to emit Radio Frequency (RF) energy is permitted to be installed in the Customer Space or to be operated within the facility without express written consent of Logista.

2.8. No device that is specifically designed to emit an electrical control signal on either AC or DC power lines is permitted to be installed in the Customer Space or to be operated within the facility without express written consent of an authorized Logista representative.

3. Customer Equipment

3.1. Equipment Delivery & Storage

Logista will accept delivery of and store customer's equipment in accordance with the guidelines set forth below. Due to limited storage space in the facility, Logista, at its sole discretion, has the right to deny or limit the amount of storage space and storage time to customers.

3.2. Delivery Scheduling

Customer shipments must be scheduled at least 5 business days in advance with Logista's Network Operations Center (NOC), reachable toll-free at (888) 292-7643 Opt 3. If Logista has not been notified of equipment arrival, we will deny acceptance of shipment.

All equipment must be delivered to the loading dock on the Monroe Street side of the Dexter Avenue Building (445 Dexter Avenue Montgomery, AL 36104). Gate entrance to the loading dock is enforced at all times and clearance must be obtained prior to driving up to the dock. Delivery trucks will be inspected and provided clearance by the dock master.

3.3. Third Party Equipment Delivery

If the equipment is delivered by a third party freight carrier, facility personnel will receive it on behalf of Customer, provided that Customer pre-scheduled the delivery with Logista.

Include the following packing and shipping information:

- Customer Name, Address, Contact Name and Phone #
- Pre-assigned Customer Rack or cage number

- Special instructions

Customer shall prepay all shipments, freight, packages, etc. Logista will not accept shipments that require any payment, whatsoever. Customer is responsible for all shipping and/or freight claims. If the shipment is large and cannot be easily brought in to the Data Center, then it is the responsibility of the customer to have the shipping company bring the equipment into the Data Center from the building loading dock.

3.4. Upon receipt of Customer's equipment, Logista will provide the following:

- Conduct a thorough visual inspection of the external packaging for possible damage.
- Inventory all boxes and verify that the carton count matches shipping receipt.
- Store the equipment in a secured area until Customer's Space is ready or available in accordance with the equipment storage policy.
- Notify Customer of receipt of all shipments, damages, or shortages, if any.
- In the event of damaged external packaging, accept the equipment and indicate, "damaged shipment/freight" on the shipping receipt and request the delivery driver to countersign acknowledging delivery of "damaged shipment/freight."
- In the event of a discrepancy, accept the shipment and indicate "short shipment/freight" on the shipping receipt and request the delivery driver to countersign acknowledging delivery of "short shipment/freight."

3.5. Equipment Storage Policy

If Customer's equipment can be safely locked in the Customer's Rack, no storage charges will apply. However, once the initial customer build has been completed no spare equipment can be stored in cardboard boxes within the confines of a customer's rack space or any portion of the colocation floor. If there is not enough storage area in a Customer's Space, Logista will store Customer's equipment in a designated and secure storage area if there is space to do so (at the discretion of the site Operations Manager).

Customer will have five (5) business in which to retrieve its equipment from the storage area from the date the equipment was delivered, after which, storage fees will apply.

All equipment left in the storage areas for more than thirty (30) days will be shipped to a Customer specified location at Customer's sole cost and expense.

Logista is not responsible for loss or damage to Customer equipment stored in the facilities or in transit if returned to Customer.

3.6. Inventory of Equipment

Logista requires an inventory of Customer equipment configuration(s) prior to execution of a colocation agreement. Logista has the right to conduct, upon reasonable advance notice to Customer, an inventory of Customer's equipment and equipment configurations during the term of Customer's license. Customer is required to obtain pre-approval for changes in equipment, including, but not limited to, upgrades, reconfigurations and removals.

3.7. Installation

Customer is solely responsible for any connections inside Customer's Space between the demarcation equipment and Customer's equipment. All wiring, connections, circuitry and utility ports shall be labelled to include appropriate information in accordance with Logista standard procedure for identification purposes.

All cables, interconnections, demarcation equipment and wiring must be cleanly wrapped and tied together and kept within the applicable cabinet or rack in a manner satisfactory to Logista. Upon request and for a fee, Logista can assist with cleanly wrapping wiring, interconnections, Customer demarcation equipment wiring or cables through our Smart Hands service. Customer shall not permit any wiring, interconnections, Customer's demarcation equipment connections or cables to enter any other space outside of Customer's rack or Customer licensed Space. Customer shall not install any equipment that cannot be securely affixed or bolted into a cabinet or rack in a manner reasonably acceptable to Logista. Customer shall not stack or rest any equipment on any other equipment. In addition, nothing may be mounted on cage walls that may restrict the airflow through the facility.

No equipment shall be placed directly on the floor. The equipment shall be at least 6 inches off the floor using either shelves or rack rails. No other method shall be used. (i.e. Cardboard boxes to elevate equipment).

In order to control deliveries, confirm the accuracy and condition thereof, and prevent subsequent loss or theft thereto, authorized datacenter users must enter the facility through the main entrance elevators and possess access

to sixth floor by swiping at the elevator. At that point they will go through standard security checks to get onto the floor. Once on the floor they may obtain access to their equipment or cargo from the security station. Tenants are not allowed on the freight elevator. Only approved personnel may have access to the sixth floor freight elevator. Logista reserves all rights to inspect incoming cargo or equipment.

For the security and safety reasons, ingress stairwell access is prohibited to the sixth floor.

4. Services Acknowledgement

Once the Colocation Services Agreement has been executed, Logista will issue a communication to the customer acknowledging the targeted installation date. This date indicates when the customer space and services are "customer ready". The date also represents the date that monthly recurring billing will begin, regardless of whether Customer actually occupies the Space on that date. Orders may have more than one TIC date for Space and power. Logista deployment specialist may engage Customer during the installation planning stage at which time mutual tasks, responsibilities, and timeframes will be identified and committed with regard to the date. Cross-connects will be billed when installed. Logista will not be responsible for delays of the date caused by Customer, or others outside our control upon which the target installation date is dependent.
Customer can request one-time services such as smart hands, by calling Logista Network Operations Center. Once a month, Logista will invoice the customer for all fees associated with service requests performed during the prior month.

5. Security Procedures

5.1. Issuing Office

The Retirement Systems of Alabama (RSA) Datacenter Security Team (DCST), is responsible for issuing all security badges, authorization forms and hard keys through its DCST office. DCST is the security liaison between the RSA and its co-location customers for access into the datacenter. DCST is responsible for the management of all active and inactive records of authorized security badges and management of the biometric security system. All records are maintained according to the RSA Records Management retention schedule assigned by the RSA to the DCST office.

Modifications to new or existing access must be submitted in writing to the DCST and approved by both the DCST Security Officer. A form entitled "Datacenter User Access Request Form" shall be provided by Logista and submitted to the DCST for approval.

5.2. Communication of Security Policy

All authorized colocation tenant contractors who have approved, unescorted access into the Data Center must read and understand this policy and ensure that they, and all workers associated with them, are compliant with this policy at all times.

5.3. Security Badge Sponsors

Responsibilities of the badge sponsor include, but are not limited to, authorizing badge requests, reviewing badge access, and requesting badge expiration extensions. For co-location tenants, the unit head (or unit head's designee) will act as the badge sponsor.

5.4. Types of Security Badges

DCST is responsible for activating, making any access modifications to, and terminating all security badges and biometric datacenter access. There are four types of security access: permanent employee; temporary; escort-only; and visitor.

Permanent Employee Badges: Employee security badges and biometric enrollment profiles are configured for co-location customers with long-term agreements. Permanent employee security badges display pictures of the badge holder for identification.

Temporary Badges: Temporary security badges are issued as replacements for lost or damaged permanent badges, and are only issued to pre-existing, approved, permanent badge holders. When a temporary security badge is issued, all policies and procedures remain in effect (including biometric access). Temporary badges are activated for

a 24-hour period. Temporary badges must be returned to DCST at or before the end of the activation period. Requests for extensions will be reviewed on a case-by-case basis.

Escort-Only (E) Badges: Escort-only badges are assigned to co-location employees who do not have permanent or temporary security badges, but must perform maintenance or service in the Data Center. Escort-only badges do not grant badge reader access to any datacenter, and the badge holder must be accompanied by a pre-approved escort at all times. Escort-only guests are not enrolled into the biometric fingerprint system. When an escort-only badge is issued, all policies and procedures remain in effect. Only authorized co-location customers who possess authorized access may escort other staff, contractors or vendors into a datacenter. Escort-only badges must be returned to DCST before the badge holder leaves the premises.

Visitor (V) Badges: Visitor badges are issued to all guests who have been pre-approved for datacenter tours or site visits. Visitor badges do not grant badge reader access to any datacenter, and the badge holder must be accompanied by a pre-approved escort at all times. Visitors are not enrolled into the biometric fingerprint system. Only authorized co-location customers who possess authorized access may escort visitors around the perimeter shells of the datacenter facility. Visitors are not allowed into any interior part of a datacenter but can observe from the glass viewing areas. When a visitor badge is issued, all policies and procedures remain in effect. Visitor badges must be returned to DCST before the badge holder leaves the premises.

5.5. Obtaining New Permanent Security Badges

In order to be granted datacenter access, the applicant's badge sponsor must complete a Datacenter Access Request Form and the Background Check Authorization and Liability Release Form from DCST. These additional forms are available from Logista upon request. DCST will process each security badge request, and upon approval will contact the applicant to arrange an appointment for a badge photo (if required) and issuance of the badge.

5.6. Controlled Key Access

Key access to racks is managed by the DCMT. Tenant access is controlled by HID card readers. In the event of a power or hardware malfunction, the DCST will work with tenants to ensure accessibility to their rack units but will not grant access to keys unless approved by the DCMT.

Applicants must present government-issued photo identification and allow for the verification of the name and identity of the badge holder. For applicants of permanent badges, a successful background check is a prerequisite for datacenter access.

Access Disqualifiers:

1. Any theft conviction.
2. Any felonious conviction within the past (5) years.
3. Any misdemeanor drug arrest within the past (2) years.
4. Any arrest involving fraud or identity theft.
5. Any arrest, discharge, resignation from a former employer for any form of cyber or computer related crime or accusation.
6. Any other incidence reflected on the report that the DCMT believes, in its reasonable discretion, should disqualify the applicant from entry into the datacenter facility.

The DCMT reserves the right to deny entry into the datacenter facility to anyone who has committed one or more of the above listed disqualifiers.

For co-location tenants, all applications for datacenter access must undergo a thorough nationwide background check (at customers expense) performed by the RSA's DCST. The applicant must possess a clean criminal history background. A sample for background checks conducted by RSA may be found at this website: Alabama Background Check System: http://background.alabama.gov/.

Access Disqualifiers:

1. Any theft conviction.
2. Any felonious conviction within the past (5) years.
3. Any misdemeanor drug arrest within the past (2) years.

4. Any arrest involving fraud or identity theft.
5. Any arrest, discharge, resignation from a former employer for any form of cyber or computer related crime or accusation.
6. Any other incidence reflected on the report that the DCMT believes, in its reasonable discretion, should disqualify the applicant from entry into the datacenter facility.

Any request for exception to this procedure must be in writing from the badge sponsor, and will be reviewed on a case-by-case basis.
Any authorized user who allows another individual to use his or her security badge will be banned from the center.

5.7. Obtaining Replacement Permanent Security Badges
Damaged Badge: Requests for replacement of a damaged badge will be processed within two working days of receipt of the request by DCST, unless a new badge photo is required. The badge holder must turn in the damaged badge to DCST before a replacement badge will be issued. If required, a temporary badge will be issued until the replacement badge is ready.

Lost Badge: Requests for replacement of a lost badge will be processed after a two-week waiting period from the time of request to DCST. The waiting period allows for the possible return of the original badge. The requesting person must submit an incident report for the lost badge to DCST before a replacement badge will be issued. If required, a temporary badge will be issued until the replacement badge is ready.

New Photo: A new photo is mandatory for any damaged or lost badge that is three or more years old. In these instances, a photo appointment must be scheduled, and the badge will be replaced at the time the photo is taken.

5.8. Obtaining Temporary, Escort-only and Visitor Security Badges
All temporary, escort-only and visitor security badge requests must be accompanied by the required RSA form, available from DCST. Applicants must present government-issued photo identification to DCST, and allow for the verification of the name and identity of the badge holder.

For all temporary security badge requests, the existing, approved access of the badge holder will be assigned to the temporary security badge. Temporary badges are activated for a 24-hour period. Requests for extensions will be reviewed on a case-by-case basis.

Temporary, escort-only and visitor security badges are only available for issue Monday – Friday, during the normal business hours of the DCST office. Contact Logista to make arrangements for temporary badges, escort-only and visitor security badges.

All visitors and escorts must fill out the required fields on the visitor and escort sign-in form located in the DCST office prior to obtaining the security badge.

5.9. Deactivation and Return of Security Badges and Biometric Profiles
Badge Deactivation: Any change in a badge holder's status must be reported to DCST. If a badge holder no longer requires access to the datacenter due to a change in status, DCST will immediately deactivate the badge and biometric profile. When an employee who has access to RSA facilities is terminated, RSA must be notified no later than 4 business hours following such voluntary termination or immediately if termination is involuntary by calling 334-517-7600 or email dcst@rsa-al.gov.

Badge Return: Security badges for access to a RSA datacenter are property of the RSA and must be returned to DCST upon deactivation due to changes in the badge holder's status. Examples of status changes include, but are not limited to: termination of employment, termination or expiration of contractor agreement, retirement, extended family leave, or transfer to another department.

5.10. Badge Audits and Access Reviews
Badge audits and access reviews will be conducted by DCST according to a predetermined schedule, based on the badge type:

Co-location Customers and Co-Location Contractors: Semi-annually (every six months)
Contractors: Semi-annually (every six months)

Notification Date: Upon issuance of a badge, a notification date and time will be entered into the DCST database, indicating the due date of the review process.

Badge Extension and Access Review: DCST will send notice to the badge sponsor no later than two weeks prior to a badge expiration date. The sponsor must confirm that the badge holder continues to need access, and that the badge continues to be in his/her possession. The sponsor must respond before the badge expiration date. If no response is received, the badge and biometric profile will be allowed to expire.

Access Extension and New Notice: After receipt of confirmation from the badge sponsor, DCST will extend access for the badge holder and set new expiration and notification of review dates accordingly.

Loss of Badge/Replacement Badge: If the badge sponsor cannot confirm that the badge holder still retains possession of the badge, access will be discontinued immediately. Upon request from the badge sponsor, DCST will issue a replacement badge, and set new expiration and notification of review dates accordingly.

Sign-in/out Registry Form: All non–RSA personnel including but not limited to contractors, co-location customers and others who have authorized access into the datacenters must fill out all of the fields on the sign-in/out registry form provided by DCST. This sign-in/out registry form will be located just outside the entry door or just inside the entry door of each datacenter.

A security badge assigned to an individual is nontransferable and may not be used by anyone other than the assigned badge holder.

5.11. Unauthorized Photographic Equipment
Cameras or any photographic equipment, including cell phone cameras, are not allowed within any Datacenter, network routing center, or leased space containing operational computing, telecommunications or network equipment.

Exceptions to this policy will be evaluated on a case-by-case basis, and any granted exceptions will require preauthorization by a RSA unit head (or the unit head's designee). In such an instance, all photographs must be reviewed and approved by the Datacenter Security Manager prior to leaving the facility.

5.12. Data Center Tours or Site Visits
Approval Process: Tours and site visits to the Datacenter are granted only under limited circumstances. All tours and site visits must be pre-approved by RSA's DCMT who will notify security. Requests for site visits or tours of the Datacenter must be submitted in writing to the DCMT and RSA Security. The DCMT Manager will review the request and send it to the unit head for approval. All requests must include the following:

1. Reason for visit
2. Number of visitors
3. Name of visitor's company or organization
4. Day/time of visit
5. Name of each visitor

Tours may be scheduled only on Tuesdays and Fridays from 2 to 4 PM unless otherwise approved by the DCMT.

Escort Assignment: Upon approval of a request, an escort from either the DCMT or the DCST team will be assigned to lead the tour or site visit.

6. Change Orders

Changes to an executed Colocation Agreement must be made in writing using the appropriate Addendum or Change Order Form and submitted to Logista. Any changes made to the initial Order Form may cause serious delays and change fees will apply. Installation fees associated with a Change Order are due and payable when the Change Order is submitted to Logista.

7. Confidentiality

Logista maintains the confidentiality of Customer's identity within the colocation facility, including, but not limited to the location of Customer's equipment. Customer may not post any signage in the facilities, including Customer cages or cabinets. Customer may, at its discretion, and provided Customer completes the required documentation, have its name displayed on approved customer signage.

8. Inappropriate Uses

Inappropriate uses include, but are not limited to activities such as unauthorized distribution or copying of copyrighted software, violation of U.S. export restrictions, harassment, fraud, trafficking in obscene material, drug dealing, and other illegal activities.

9. Sites Not Welcome at Logista's Data Center

Logista forbids hosting websites that contain hatred messages including racism, sexism, or sites promoting one particular race, sex, or nationality as superior and/or another race, sex, or nationality as inferior inside the data center. Websites that promote activities that violate federal, state, local laws and/or violation of U.S. export restrictions are also not welcome. Logista will report and take immediate action towards anyone violating U.S. laws, including providing logs and related account information that may be used against the offender in court proceedings.