ACD.net DATA CENTER PHYSICAL ACCESS POLICY

THIS AGREEMENT is made on this _____ day of _____, _____, between name: _____, with the organization:_____, business address _____ (hereafter referred to as “the Undersigned” or “Customer”) and ACD.net (hereafter referred to as "Company").

The purpose of this policy is to set forth the ACD.net Data Center Physical Access Policy (“DCPAP” or “Access Policy”) by which the undersigned will abide while using, renting, leasing, or otherwise making use of Company facilities, goods, and services (“Data Center or Contracted Spaces”). By using Company’s Data Center and facilities, the undersigned agrees to comply with the following policies.

Terms and Conditions

As a service, the standard Data Center Access and Security Policy is provided below.

1. Company and Customer Responsibility.

The Data Center is intended as a limited physical access location for servers. Systems administrators of machines which are housed in the Data Center should plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements. With this in mind, it is highly recommended that all servers be configured with secure access administrative tools to allow for remote maintenance. All machines in the Data Center must be rack mountable, unless prior arrangements have been made to allow particular non-rack-mountable hardware into the Data Center. Certain machines which have a business need to be in the Data Center and currently are not rack mountable should be replaced within a reasonably short time period of time with more appropriate hardware, or the machines’ functions need to be relocated to other servers which are more appropriate for the Data Center.

Company is responsible for ensuring that all resources under its control remain physically secure. The Company maintains this access policy to provide a framework for Customers to follow for physical security and access to Company facilities and to instruct Customers on the procedures and policies that Company staff and technicians follow. Undersigned agrees to adhere to all posted notices or changes to protocol that the Company makes the Undersigned aware of during its visits to Company facilities.

2. Data Center Policies

Access into Company facilities requires adherence to the following protocols and restrictions on dangerous materials (“dangerous materials”):

- No smoking or chewing tobacco is allowed.
- No combustible materials may be brought into the data center, including lighters, hand-warmers, mace, tear gas, aerosol cans, or compressed air.
- No eating or drinking is allowed in the data center.
- No drugs or alcohol are permitted in the data center.
- No weapons or firearms are allowed in the data center.
- No external fire suppression devices are allowed.
- No prohibited hardware is allowed. All work-related materials must be cleaned up before leaving.
- All work-related trash or garbage must be disposed of properly.
- No illegal activity of any kind is permitted.
- Unattended equipment and/or supplies outside of customers rack will be disposed of without notice.
- Doors will remain closed at all times except for entrance and egress.

3. Access Keycards and Identification.

Company will issue secure access keycards to Undersigned and Undersigned's designated agent(s). Company shall maintain a list of all authorized personnel issued such access and at no time shall secure access keycards transfer between any other employee or other agent of the Undersigned without pre-approved, written permission from Company. If at any time, Company becomes aware that an access badge has been transferred in violation of this policy, revocation of access to the Data Center and contracted space(s) may occur.

4. Data Center Access Procedures.

Access to the Company Data Center without a valid security card requires that all Customers present valid id and sign in with a valid signature for a Company staff member to grant them access.

Customers accessing the data must have their identification and security card available for inspection at all times.

Failure to adhere to the sign-in and sign-out procedures could result in revocation of access to the space.

4.1 "Visitor" Physical Access and Procedures.

Visitor shall mean any individual who is not on an approved Access List on file with the Data Center. All visitors shall enter the Data Center through ACD.net's Welcome Area and wait for a Staff Member to sign the visitor in.

The Undersigned may allow Visitors to gain access to the Data Center, subject to the Undersigned's Access Type, provided that:

1. All visitors must have their visit(s) scheduled and approved by the Company Data Center Supervisor at least 24 business hours prior to their visit.
2. All visitors shall sign a copy of the Data Center Physical Access Policy ("DCPAP") to be kept on file by the Data Center and shall be governed according to the Specifications of the Data Center Contract or Co-location Contract between Company and Undersigned.
3. A Data Center Employee or Staff Member must accompany Visitor(s) at all times while within the Data Center.
4. All visitors must sign in and sign out when entering or exiting the Data Center. Visitors must wear an identification badge at all times.
5. Upon sign-out and exiting the data center, visitors are responsible for turning in any identification badges or ID issued to them during their visit. Failure to properly turn in these materials may result in financial penalties or sanctions against Undersigned or Visitor.
6. Any exceptions to any of the above policies must have the written approval of the Data Center Supervisor.

4.2 Disclosure of Security, Access, or other Policies Governing the Security of the Data Center.

All persons entering the Data Center, whether the Undersigned, its Agents, Employees, Vendors, or Visitors agree to hold all Information Proprietary, including all information related to the security, operation, policies, procedures, or any an all other information they may come in contact with, including other customer information. No less than reasonable care shall be maintained by the Undersigned or its agents.

Undersigned agrees not to disclose or use any such Proprietary Information or any information derived from Data Center contact to any firm, supplier, business, individual, third party, or other organization without written consent directly from ACD.net.

5. Data Center Access Types.

For our customers' convenience, the Company maintains several types of access to the Data Center.

Access levels include:

5.1 Unrestricted Access
24 x 7, 7 Days a Week Access

5.2 Restricted Access
8am - 5pm, M-F Access

5.3 Escorted Access to Contracted Space(s)
No charge during business hours by appointment

The level of access shall be determined and maintained by the Company and Customer according to the Specifications of the Data Center Contract or Co-location Contract between Company and Customer.

6. Emergency Access by Personnel Not Currently on Access Lists.

Access by Undersigned or Undersigned's Agents not currently on any access lists may be granted only by the Company Data Center supervisor and shall be governed according to the Specifications of the Data Center Contract or Co-location Contract between Company and Customer. Access to the Data Center under this condition shall be noted as an "emergency access" in the Data Center security logs. Any inappropriate use of "emergency access" may result in access being immediately denied and the requesting Undersigned or Undersigned's Agent being ejected from the Data Center and/or Customer's "emergency access" privileges revoked.

7. Modification of Agreement.

Company reserves the right to add, modify, or delete any provision of this Agreement at any time and without notice. Company reserves the right to restrict any access right at any time, whether a violation of this agreement occurs or not. Company reserves the exclusive right and will be the sole arbiter as to what constitutes a violation of any of these provisions.

8. Potentially Tortuous or Illegal Conduct.

The following shall be construed as violations of this Agreement and may result in suspension or deletion of a Customer's account or in termination of this Agreement:

a) Falsifying any information provided to Company or to other staff members in connection with access to the data center or the use of a Company facility, product, or service.
b) Allowing access to any restricted area(s) by individual(s) or allowing individuals to gain access to any restricted areas as defined in the Specifications of the Data Center Contract or Co-location Contract between Company and Customer.
c) Allowing any dangerous or restricted materials inside the data center or Company facilities at any time.

9. Additional Equipment Beyond Initial Deployment.

All new systems and hardware to the Data Center will need to be coordinated and scheduled with Data Center staff. As the number of machines in the Data Center grows, the infrastructure that supports the entire Data Center must incrementally expand. Sometimes this may mean a small delay in the deployment of hardware into the Data Center until we have the appropriate infrastructure (including console, network, power, and rack space) for the hardware to be deployed.

10. Data Center System and Network Security.

Violations of Data Center system or network security are strictly prohibited, and may result in criminal or civil liability. Examples include but are not limited to: allowing unauthorized access to data center; use of any Company product or service that Customer does not have permission to use; use of any equipment, hardware, connections or other materials that Customer does not have permission to use; disruption or interference with the connectivity and access or otherwise impeding other Customers' use of or equipment within the Data Center, products, or services.

11. Consequences of Violation.

If Company becomes aware of an alleged violation of any of the terms contained in this Agreement, or any other policy that has been posted on its web site, made available to Customer via email, or posted in any other form, Company shall initiate an investigation. During the investigation, Company may restrict Customer's access to the Data Center or other Company products and services to prevent further possible unauthorized activity. Company may, at its sole discretion, restrict, suspend, or terminate Customer's account without notice or refund, or pursue civil remedies as it deems necessary. Company shall notify the appropriate law enforcement department of any such violations. Company shall not be responsible for any payment, refunds, or compensation in any way for service disruptions or termination resulting from violations of this Agreement.

12. Initial Cards and Replacement Cards

The number of included security cards varies by the amount of space utilized by Customer.

Rack Space	Qty Cards	Cost for Additional Cards (per)
Full Rack	3	$10.00
Half Rack	2	$10.00
Below Half Rack	1	$10.00

Replacement for lost cards are $10.00.

The Undersigned represents and warrants that, on the date first written above, the Undersigned is authorized to enter into this Agreement in its entirety, and duly binds its respective principals by the signature below.

EXECUTED as of the date first written above;

_____

By: _____

Title: _____

Date signed: _____