



## Managed Data Solutions NOC Access Control Policy

Updated 6-4-2007

Access to the Managed Data Solutions Network Operation Center(s) (“**NOC**”) is restricted, and is governed by this NOC Access Control Policy (“**ACP**”). At no time will deviations from these policies be allowed. Only the security officers of Managed Data Solutions, LLC (“**MDS**”) will make changes to these policies. This policy defines the physical security, integrity, and access to any hardware housed in a Managed Data Solutions, LLC, NOC. No other document, policy or action shall serve to define or deviate from this policy.

**Restricted Access:** MDS Security Officers are the only persons explicitly allowed to enter any MDS NOC. At the sole discretion of one or more MDS Security Officers, restricted access to an MDS NOC *may* be granted to the owner or owner’s representative of a colocated server or dedicated server or other customer owned hardware housed in an MDS NOC during our normal business hours. Access to the NOC requested by the customers, not during our normal business hours may be subject to a service fee. Restricted access to an MDS NOC will only be granted after MDS Security Officers review and approval the previously supplied credentials each time access is requested.

**Limitations:** Access to any hardware, software or any other equipment housed within an MDS NOC is restricted to an MDS Security Officer, or where appropriate, the authorized representative as listed below, or the owner of said hardware. At no time will access be allowed regarding any other hardware or equipment in an MDS NOC. At all times while in an MDS facility, any person granted restricted access to an MDS NOC must abide by all local, state, and federal laws and regulations, as well as the policies as defined in this Policy.

**Responsibility:** Any person granted restricted access to an MDS NOC, and the company, organization, or agency represented by this person, are completely and wholly responsible for their actions while they are a guest in an MDS NOC. Damages or other resultant legal action may be brought against any person, company, organization, or agency whose representative violate any MDS policy, or any local, state or federal law or regulation. At any time an MDS Security Officer witnesses or discovers illegal or inappropriate activity of any person in any MDS facility, including a NOC, the appropriate law enforcement agencies will be notified immediately.

**Credentials:** Acceptable photo identification must be carried at all times while in an MDS NOC. Acceptable photo ID’s must be approved by an MDS Security Officer, prior to being granted restricted access to an MDS NOC. Acceptable and Unacceptable forms of ID are as follows:

Acceptable

- Valid State Drivers License
- Valid State Photo Identification
- Valid military or federal agency photo ID
- Valid US Passport

Unacceptable

- Visas
- Bank cards
- Credit Cards
- Telephone Cards

**Assignments:** The owner or security officer of any colocated or dedicated hardware shall name below those persons they wish to allow access to an MDS NOC. No other person shall be granted, at any time, for any reason, access to an MDS NOC or any equipment located within an MDS NOC. This policy must be signed and dated by the owner or security officer of the colocated or dedicated hardware located in an MDS NOC. Copies of valid photo identification, must accompany this policy for the owner or security officer of said hardware, and for each person for whom restricted access is requested. This policy will remain on file permanently at a Managed Data Solutions facility, and is the property of Managed Data Solutions, LLC.

**Identification:** Prior to authorized restricted access entry to an MDS NOC, previously approved photo identification must be presented to and approved by an MDS Security Officer. This photo identification will be compared to the identification maintained on file by MDS. Other forms of identification may be utilized by MDS, including retinal or fingerprint scanning technologies.

**Notification:** Restricted access to an MDS NOC requires a notification period of at least one hour. This ensures an MDS Security Officer will be available to provide approval and restricted access at the time you require during normal business hours. In an emergency situation, an MDS Security Officer may accommodate access with less a less than a one hour notification period. The nature of the emergency and other factors will be considered in this approval process. Access outside of normal business hours will be addressed at the time the request is made.



**Managed Data Solutions NOC Access Control Policy**  
Updated 6-4-2007

**Monitoring:** MDS Security Officers will monitor all MDS NOC activity. The forms of monitoring may include video, audio and motion surveillance, physical surveillance, or other forms of monitoring and recording.

**Terminations and Changes:** Any change to the authorized persons list below is the sole responsibility of the Security Officer of the organization shown below. The only notification that will be accepted by MDS is a signed, dated letter from the Security Officer listed below on company letterhead. This letter can be faxed, but must be followed as soon as possible by a signed original copy of the letter. MDS reserves the right to terminate any restricted access, for any reason at any time, and without notification. Payment default or contract termination will result in the immediate cancellation of restricted access to any MDS NOC as defined in our Managed Data Solutions Hosting Services General Terms and Conditions document that is a part of this policy, and can be found within our web site located at <http://www.mdatasol.com>.

**Sign In / Sign Out Procedures**

Before being granted access to an MDS NOC, any guest must be authorized by a Security Officer, and approved by an MDS Security Officer. Proper photo identification must be presented to an MDS Security Officer prior to restricted MDS NOC access being granted. The MDS NOC guest must sign in using the MDS NOC access log. Upon photo ID inspection, and approval by the MDS Security Officer, the guest will be provided physical access to the appropriate hardware in an MDS NOC. Upon leaving the NOC, the guest must sign out using the MDS NOC access log.

**NOC Restricted Access Request**

By signing below, I certify that I am the Owner or Owner's designated Security Officer responsible for the hardware and other related equipment and the organization also named below. I further certify that I have read, and understand the MDS Photo ID Policy, and agree to be bound by its terms.

Organization	Owner / Security Officer
Date	Owner / Security Officer Signature

**Authorization List**

The following persons are authorized by the above named Owner or Security Officer shown above to gain restricted access to their equipment in an MDS NOC. Each person agrees to be bound by the terms of the MDS Photo ID Policy and this policy.

Name	Signature	SSN	Date	MDS S.O.