Physical Security & Access Control Policies

Physical Security

Nebraska Data Centers takes security as a vital component of our data center services. The procedures as outlined in this document have been developed to establish policies to maintain a secure Data Center environment. It is important that all employees, vendors, customers, contractors and authorized visitors of NDC comply with these policies.

The security within our facilities involves multiple layers of access while also providing the convenience of 24/7/365 access to our authorized customers. Our security involves the following features:

1. Building Perimeter Monitoring – with video cameras on doors and surrounding areas
2. Guard Station – with ID verification, and login policies for building guests and vendors
3. Indoor Monitoring - 24/7 video of all indoor spaces and suites
4. Proxy Card Building Access – Secured doors require proxy card to enter
5. Elevator Proxy – Floor access is controlled through the proxy to restrict inside access
6. Man Trap Proxy – Access to the data center hallways requires another layer of approval
7. Dual Factor (Proxy and Fingerprint) required for data center suite access
8. Cabinet / Cage Access – Combination lock or better

Access Control Policy and Procedures

**Primary Guidelines** - The “Data Center” is a restricted area requiring a much greater level of control than typical spaces. Only those individuals who are expressly authorized to do so by NDC may enter the area. Access privileges will only be granted to individuals who have a legitimate business need to be in data center.

All customers sharing the Data Center will familiarize themselves thoroughly with this document. Any questions regarding policies and procedures should be addressed to NDC Operations by calling 402-342-2656 or emailing noc@nebraskadatacenters.com.

The only exception allowed to the Data Center Security Policies and Practices is the temporary suspension of established rules if it becomes necessary to provide emergency access to medical, fire and/or police officials, etc.

**Levels of Access into the Data Center** - There are multiple “Levels of Access” to the Data Center – Controlled Access, Escorted Access and Temporary Access.

**Controlled Access** is given to individuals who have access authority into the Facility, into the elevator and into the authorized Data Center space. Controlled Access is granted to the individual whose job responsibilities require that they have access to the specific designated areas within the facility.

*Any violation of the policies as outlined in this document by customers, employees, contractors and vendors may result in temporary and/or permanent suspension of access privileges or, when appropriate, legal action. For vendors and contractors, violation of security procedures is grounds for contract termination and immediate dismissal from the property.*
A person provided Controlled Access will have access into the facility, elevator and the data center on a 24/7 basis. These individuals will be registered in the NDC security system, the building security system and will be provided Customer Badges that will be uniquely assigned to them. The controlled access begins with entrance doors as well as the elevators. During normal business hours, these Customers will be allowed to enter the front door and back doors. If they enter the front door of the Omaha facility, the Security Officer may ask for them to provide identification and badges.

**Escorted Access** is closely monitored accesses given to people who have a legitimate business need for infrequent access to the Data Center. “Infrequent access” is generally defined as access required less than 4 times a year. Individuals with Escorted Access will not be issued badge access via NDC Operations.

A person provided Escort Access is required to sign in and out under the direct supervision of an NDC Operations employee. The individual must provide positive identification upon demand and must leave area when requested to do so.

A person with Escorted Access to the area must not allow any other person to enter or leave the area.

**Meet Me Room (MMR) Access** is only available via Escorted Access. All request to enter the MMR must be done by emailing the NDC NOC at noc@nebraskadatcenters.com. All requests must be received 48 hours in advance of required access.

**Temporary Access** It is policy of NDC Operations not to issue access cards to the Data Center for temporary access purposes. Request for exceptions to this policy will be considered on a discretionary, case-by-case basis. If NDC Operations issues an access card to an individual, the individual may not share, loan or copy the access card. Only those granted Controlling Access can request and be issued an access card which only will be granted on a limited, justifiable basis.

NDC Operations performs the actual physical management of badges and access cards for the Data Center Areas.

### Access List Management

**Managing Access to the Data Center** - Customers with equipment in the Data Centers may request access to the Data Center. The individuals designated by the requesting customer shall be granted access once NDC completes the authorization process. To initiate authorization for access, customers should submit the “Access List Management” form (Appendix B) to the NCD NOC at noc@nebraskadatcenters.com.

Upon receipt of the notification to request access approval, NDC Operations will schedule an appointment with the individual requesting access. During this onsite visit, the individual or individuals will review the NDC Data Center Access Policies and be asked to sign a “Data Center Access Agreement” (see Appendix A). A copy of the completed Agreement will be given to the requestor for proof of authorization and the original document will be maintained on file at NDC. Once the agreement is signed, NDC Operations will administer the access process by securing a unique proximity card and fingerprinting the individual for biometric access.

If for any reason, individuals who have been granted Controlled Access no longer needs or warrants access,

**Termination of Access** It is the responsibility of the Technical Contact as noted in the NDC MSA and or primary contacts contractor to notify NDC as soon as possible of the change in access status by submitting the “Access List Management” form. NDC will then terminate access privileges for that individual until further notice. This is extremely important in cases where the employee was terminated for cause.

Additionally, periodic (at least annually) reviews will be performed with any level of access to the Data Center by NDC Operations. As part of that audit, customers will receive a list of all individuals with approved access. If an individual no longer requires Data Center Access it will be revoked at this time.
**Access Control Log**  The Data Center Access Control Log is managed by NDC Operations staff and kept in the NOC. All individuals with Controlled Access to the Data Center are responsible for ensuring that they have contacted NDC when providing Escorted Access. The following procedures must be followed.

Each time an individual with Escorted Access to the Data Center is admitted to the area, he must properly log in on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form.

Each time an individual with Escort Access leaves the area, he must properly log out on the Access Control Log at the time they leave (even for a short time). The person with Controlled Access to the area who allows the visitor to leave must make sure to fill out the log when the Escort leaves the facility.

**Exception Reporting**  All infractions of the Data Center Physical Security Policies and Procedures shall be reported to NDC Operations as soon as possible.

Should an unauthorized individual be found in the Data Center it must be reported immediately to a member of NDC Operations. If this occurs after business hours, the Operations Manager should be contacted at 402-342-2656. The unauthorized individual will be escorted from the Data Center immediately.

Any forcible or improper entry into the Data Center should be immediately reported to NDC Operations, which shall deal with the situation expeditiously.

Individuals with Controlled Access should monitor the area and report any individuals who appear to be compromising either the security of the area, the activities, or disrupting the operations. It is particularly important that individuals with Controlled Access show initiative in monitoring and maintaining security of the Data Center.

**General Data Center Operations Policies for Customers**

All authorized personnel must adhere to the latest version of Nebraska Data Center’s Security and Access Policy and Procedures document.

Customers are restricted to authorized areas only, including the lobby, conference rooms, common areas and customer space on the data center floor.

Security controls include elevator proxy cards, bio metric entrance doors, cabinet locks, sign-in procedures for all ingress and egress, managed key and access card plans and managed access permissions and access request methods.

Closed-circuit television (CCTV) cameras are used to monitor all areas of the facility's including lobbies, common areas, data center floor space, admin areas and engineering plant critical infrastructure areas for your safety. All CCTV cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.

Tampering with, or in any manner adversely affecting, security and/or safety systems within NDC is strictly prohibited.

Doors may not be propped open. These access doors are monitored and alarmed.

NDC reserves the right to access any part of the data center at any time for safety and security reasons.
All persons entering the Data Center must:

1. **Possess a valid government issued photo ID**
   - This includes a driver’s license, state-issued identification card, passport, or military identification card.
   - Identification cards issued by employers (company ID) are **not acceptable**.
   - Other forms of identification that are not issued by government agencies, such as a credit card, are **not acceptable**.

2. **Have authorization to access the facility via their respective companies Access List**