



# VAULTAS

YOUR DATA. YOUR DATA CENTER.

Minneapolis, MN | St. Cloud, MN | Alexandria, MN | Milwaukee, WI  
[www.vaultas.com](http://www.vaultas.com)

April 15, 2020

Customer Name:  
Attention:  
Address:  
City, State & Zip:

RE: Vaultas Alexandria Access Control Policy

Dear, Customer and Visitors

Vaultas Alexandria is equipped with a state-of-the-art Proxy Card Facility Access System, and 24x7x365 CCTV Security and Monitoring System. The systems provide security and functionality features to our facility. It allows us to track by individual all movement into and out of all areas of the facility. The system allows us to control all areas of the facility and provides the ability to lock down or lock out anyone at any time 24x7x365 providing for immediate response to any threat or security breach. Along with the physical systems in place we also deploy a detailed "Personal" ID Badge component so access cards cannot be shared or used by anyone but the authorized person. This helps us increase the security level of our facility significantly for the benefit of all our customers and visitors.

Vaultas Alexandria strives to achieve a difficult balance-both as a friendly and welcoming environment and, at the same time, one that is highly secure for all who use and trust our facility with their critically important data and IT equipment. This document will detail the policies and procedures that will be used to protect our organization, facility, people, and assets of us and all of our customers by controlling what and who enters and leaves any and all areas of the facility.

The following is a detailed policy document that will be reviewed and adjusted on a regular basis to provide a way to regularly monitor these policies and make any and all adjustments for the benefit of keeping our facility safe and secure for everyone who uses it.



# Vaultas Alexandria Access Control Policy

## Table of Contents

Introduction .....	Page 3
Authorized Personnel .....	Page 3
Awareness & Training .....	Page 3
User Responsibilities .....	Page 4
Other Things to Consider .....	Page 4
Building Access .....	Page 4
Vendors & Service Personnel .....	Page 4-5
Guest Policy .....	Page 5
Visitor / Vendor Form .....	Page 6

This document is intended only for the named recipient(s) and may contain confidential, proprietary or legally privileged information. No confidentiality or privilege is waived or lost by any misdirected transmission or communication of this document. If you received this document, it is your responsibility to keep this document and contents confidential. You are only authorized to share it or any of the contents on an as needed basis. If you are not the intended recipient, you must not use, disclose, distribute or copy any part of this message.



## **Introduction**

This Secure Access System is being used for the benefit of everyone. All access doors operate as “mantraps” and require certain steps to be followed in order to access the facility. Everyone who enters the facility will be recorded; this allows us to provide a higher level of security to all our customers, vendors and guests. This provides for a safe and secure environment for you, your equipment and everyone’s critical data housed within the facility. These policies need to be followed and are required by all individuals who enter and/or work within the facility. The Access Cards and ID Badges are issued to individuals and not to the company. This means whoever is issued an access card and ID badge is responsible for it and their part in the security of this facility. This is an important part that each person needs to understand and participate in, so we can maintain a safe and secure facility for all. It will be important that access cards and ID badges are not shared, lost or stolen. If they are lost or stolen it is critical that they be reported as lost or stolen to Vaultas personnel immediately, so the affected card(s) can be deleted from the system and security can be maintained. All unauthorized individuals, vendors, contractors and guests etc. must be escorted at all times within the facility. These guests, vendors and contractors are the responsibility of those who provide them access. The facility is under heavy CCTV coverage and we will have access to any information necessary to identify any breach to this policy. We here at Vaultas truly appreciate every effort you provide to maintaining the security of the facility for us and those who count on us to keep it safe and secure.

## **Authorized Individuals**

Official Vaultas staff, clients, customers, authorized vendors, contractors and visitors shall be admitted to the building without approval by the Vaultas organization. All employees who are issued an access card and ID Badge must undergo a background check before access can be granted. It is the responsibility of the customer, vendor and/or contractor to assure Vaultas that this background check procedure has been completed. If for any reason this cannot be done, please inform the Vaultas team, and we can discuss or consider Vaultas providing this service to you. It is imperative that these procedures be followed and repeated on an annual basis to assure we are providing the highest level of security for everyone who counts on us for their data security.

## **Employee Awareness & Training**

For our policies to provide effective security, all building users and occupants must recognize the importance of following and adhering to these security procedures. All staff, customers, vendors and contractors will be informed through this policy document and proceeding updates from time to time. This document can be requested from a Vaultas staff member at any time. We ask that All Vaultas staff, customers, vendors and contractors immediately report any and all suspicious activity 24 hours a day. We also encourage anyone with questions and/or concerns to contact any Vaultas staff for information and/or clarification to these policies.

## **User Responsibilities**

All users are responsible for their activities within the facility that could breach security. At no time shall anyone allow an unauthorized person use their access card or ID Badge. It is the responsibility for all card holders to report any breach in security, lost or stolen access card or ID badge. To report any unauthorized person in or around the facility. In order to maintain a highly secure and safe facility for everyone who uses it everyone MUST participate in the



security policies. There are three components to the security access system, ID Badge, Access Card and Security Access Pin Code. There are costs to Vaultas to create, document, coordinate and maintain this system for the benefit of all who use it.

There will be fees and charges associated if any of these are lost or stolen and need replacement or reset. The costs associated with these are listed below:

- **Lost or Stolen Card or ID Badge = (1 free for the 1<sup>st</sup> calendar year) after that; first occurrence \$35.00, second occurrence \$50.00, third or more \$100**
- **Additional Cards = \$35.00 (plus a completed justification form and background check)**
- **Reset of Access Pin Code = (1 free for the 1<sup>st</sup> calendar year) after that; \$35.00**
- **Penalty for sharing Access Card or ID Badge = \$100.00 or (the cost of service personnel to research and eliminate the breach)**

## **Other Things to Consider**

This document is not all inclusive and we request the use of good common sense and good judgment when working and operating within the facility. There are many other functions and services that your organization may provide that demand specific security provisions. Parking facilities, open spaces, and other physical elements require you to secure them appropriately. If your organization rents out space, has a project requiring you to enter and leave the facility often, or to bring in large amounts of equipment, or provides any other services outside of your regular use of the facility, you must plan accordingly. It may require additional persons to maintain a secure facility during these operations. Doors can “never” be propped open or left open and unattended. If you cannot provide for additional personnel required to maintain effective security, please notify and plan your work in cooperation with Vaultas staff so we can provide the assistance needed. This document is only to help you understand the needs and responsibilities of security provisions and access control policies. It should not take the place of professional security consultation and best practices used by all to maintain a safe and secure facility.

## **Building Access**

The 8<sup>th</sup> Street entrance will be the only point to enter and exit the building during normal operations. All other doors will only be used for emergency exits and are alarmed at all times. Routine and random inspections will ensure that the alarms are functioning, that the routes to the emergency exits are clearly marked and unblocked, and that exterior doors are not propped open for any reason which may allow outsiders access into the building.

## **Vendors, Contractors and Service Personnel**

All vendor or service companies must provide verification that their employees undergo background checks. Front desk staff/screeners must have a list of all contracted vendors and service personnel on hand and will require proper business-specific identification from the visiting personnel. The front desk staff should be made aware of expected vendor or service visits via the “Visitor / Vendor Form.” This form can be obtained from the Vaultas Website at [www.vaultas.com/security](http://www.vaultas.com/security).

Any and all service personnel who must be permitted access to the premises must sign in and out with the visitor logbook, located in the lobby area of the facility.



## **Guest Policy**

Any building occupant expecting a guest must notify Vaultas staff and provide the guest's information "before" the guest's arrival via a "Visitor / Vendor Form." The visitor should be informed of the Vaultas security policies and that a Vaultas staff person may require personal picture identification.

The Vaultas staff will greet visitors and ask appropriate questions about the visitor's destination in a courteous and professional manner. The Vaultas staff will contact the person being visited to verify that the guest is welcome and expected before permitting the guest access to the premises. In some instances, such as when inadequate Vaultas staff is available or Vaultas staff was not notified of the visitor in advance the staff person expecting the guest must come to escort the guest into and out of the premises. Before being permitted access to the premises all guests must present a valid ID and must sign-in into the logbook. The logbook requires the person's name, the time of arrival, who they are visiting, and the guest's signature. The guest must sign out with the front desk when leaving.

Thank you in advance for your support and attention to this and all Vaultas policies, your continued attention and support is required in order for us to operate and maintain a safe and secure facility for the benefit of all customers, vendors and contractors.

This is confidential and proprietary information intended for the use of only those authorized Vaultas customers, vendors, suppliers and contractors. Any use of this information not for the benefit of Vaultas is expressly prohibited. This information should not be shared with any un-authorized person or entity at any time.

**Visitor / Vendor Form below -**



## Visitor / Vendor Form

### Visitor / Vendor Information

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Organization: \_\_\_\_\_

ID/Driver's License #: \_\_\_\_\_

Email Address: \_\_\_\_\_

Reason for Visit: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

### Vaultas Customer Information

Organization Visiting: \_\_\_\_\_

Organization Contact: \_\_\_\_\_

Contact Telephone #: \_\_\_\_\_

Contact Email: \_\_\_\_\_

This confidential information and will not be shared except as needed to maintain a safe and secure facility for all Vaultas customers, vendors, suppliers and contractors.

**Vaultas Alexandria, LLC**