Aberrant Open-ISM™

PHYSICAL SECURITY POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 PURPOSE

It is this policy's purpose that <<Company Name>> operates within a framework that ensures that its physical locations are secure from breaches in access and that only authorized personnel have access to its facilities at all times.

This policy establishes and describes the key aspects of the administration of its physical security policy.

2 SCOPE

This document establishes the policies of securing <<Company Name>>'s physical environments including its local office.

This policy does not apply to colocation facilities, or cloud providers that host servers or virtual infrastructure.

3 ROLES AND RESPONSIBILITIES

3.1 INFORMATION SECURITY

The CISO is primarily responsible for establishing and overseeing <<Company Name>>'s policy and ensuring that the appropriate controls are being followed.

3.2 VENDORS

<<Company Name>>'s vendor relationships that host facilities in which <<Company Name>> intellectual property is stored (e.g. the company website and associated data) must have policies in place that restrict access to the facilities only to authorized personnel.

3.3 EMPLOYEES

Each employee is responsible for understanding and conforming to the policy and the risks associated with providing unauthorized access to the company's physical locations.

3.4 COMPANY OFFICE SECURITY

3.4.1 BUILDING PHYSICAL SECURITY PERIMETER

<<Company Name>>'s corporate office can only be accessed by authorized personnel through keycard access. The main floor of the building in which the <<Company Name>> office is located is staffed 24x7 by a trained security officer—24X7 video surveillance of the lobby is maintained for 30 days by building management. Access to the floors on which <<Company Name>>'s office is located is controlled by keycard access in the elevator—access to other floors in the building is restricted. Only front desk security can override elevator access. Security will only allow visiting personnel up to the <<Company Name>> floor after signing in and stating their purpose for the visit. This includes delivery personnel.

3.4.1.1 DELIVERY AND LOADING AREAS

Delivery personnel are required to check-in with the building security in the lobby prior to being given one-way access to the <<Company Name>> office via an elevator that requires a security override of its keycard access system. Delivery personnel must then 'buzz' in through a locked glass door by a <<Company Name>> employee. Delivery personnel are then escorted into the lobby where business is transacted.

3.4.2 OFFICE PHYSICAL ENTRY CONTROLS

Physical access control to <<Company Name>>'s office are operated and maintained by the InfoSec Team. Employees are issued keycards that also operates as photo identification. Use of a keycard generates an access log record that identifies the employee and is electronically stored for one year. Authorized personnel can only access the office via a keycard.

24X7 video surveillance systems are in place for all <<Company Name>> office entry points and for the network closets. Videos are actively monitored by a third party with system checks in place to verify DVR functionality and uptime. Recordings are retained for no less than 90 days with access to recordings provided upon request.

Company confidential information (e.g. financial records) are kept in locked cabinets with key access only to authorized personnel.

The network closets that house connectivity to the company's internet and corporate domain are kept locked at all times and access is granted only to authorized personnel approved by the CISO, or designated employee.

By design customer data is not held at the <<Company Name>> office. All customer data is securely located at third party data centers and accessed via remote terminals that incorporate secure transport using standards that conform to industry best practices as it relates to security.

3.4.2.1 EMPLOYEES

Employees are granted access to the facility based on management approval. Access to the network closet requires explicit permission from the CISO, or delegated employee. Employee access to the facility is reviewed periodically by management. Employee access to <<Company Name>> systems and facilities is revoked on the date of termination.

3.4.2.2 WORKING IN SECURE AREAS

Secure areas are for designated employees only. Employees performing work in secure areas should exit the area once the work is completed.

3.4.2.3 DELIVERY PERSONNEL AND VISITORS

Delivery personnel or other visitors are greeted by office personnel at the locked door at the company's main entrance. Visitors to the office must sign in at the front desk. An electronic copy of the visitor log is retained by <<Company Name>> for at least one year. Visitors must always be accompanied by company personnel and restricted from access to areas that might contain sensitive information. Access to the office and controlled spaces is reviewed by InfoSec on at least a quarterly basis.

3.4.2.4 BUILDING MANAGEMENT PERSONNEL / CLEANING STAFF

The property management team has access to the building. The team consists of a property manager, chief engineer, and tenant coordinator. Relative to vendors, the day porter and evening janitorial staff have access to the <<Company Name>> space and have all undergone criminal background checks.

3.4.3 SECURING AGAINST EXTERNAL / ENVIRONMENTAL THREATS

The fire alarm and sprinkler systems are tested at least annually by building management. Fire access doors are failsafe and designed to prevent unauthorized entry from the stairwell. Fire extinguishers should have updated inspection tags.

3.5 EQUIPMENT

3.5.1 EQUIPMENT SITTING AND PROTECTION

All personnel are responsible for the security of IT assets under their control from purchase to disposal.

3.5.1.1 SCOPE OF END USER ASSETS

All desktops, laptops, servers and other high value IT Assets (those with a unit cost of more than $5000 excluding Personnel owned End User Assets) shall be secured with a preventative physical security control to prevent loss or theft or unauthorized physical access.

3.5.1.2 THEFT OR LOSS

Users must report the loss of End User Assets to the Service Desk within 48 hours. If the End User Asset was stolen, a police report shall be provided with the report of loss to the Service Desk. Additionally, users must immediately report the loss of Network Assets to the IS team.

3.5.2 SUPPORTING UTILITIES

End user assets need to conform to the Acceptable Use Policy—this includes adherence to applicable security policies and the installation of anti-virus software. Additionally, full disk encryption shall be used on all laptops. A review of all machines on the network shall be conducted by support personnel on a quarterly basis.

3.5.3 CABLING SECURITY

Power and telecommunications cabling carrying data or supporting information servers shall be protected from interception, interference or damage.

<<Company Name>> utilizes RJ45 Cat5e Ethernet cables which are ideal for use in industrial Ethernet networking applications where EMI and RFI are present. RJ45 Cat5e Ethernet Cables feature 26 AWG stranded cable construction providing flexibility as well as a 100% foil shield and are designed to perform to EIA568 standard.

3.5.4 EQUIPMENT MAINTENANCE

In the event of a technical issue users must contact the Help Desk for support. If a vendor is required to perform maintenance on <<Company Name>> assets the vendor must be vetted and pre-approved in accordance with <<Company Name>> Vendor Management policies.

3.5.5 REMOVAL OF ASSETS

If an asset is removed from an employee it must be returned to the IS team.

3.5.6 SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES

All personnel are responsible for the security of IT assets under their control. Equipment used to support business activities off-premises must be made subject to the same type of management authorization and security protection as that of on-site equipment. Personnel are expected to take reasonable measures to ensure that equipment isn't stolen, e.g. avoid leaving equipment out in the open in their unattended vehicle, etc.

3.5.7 UNATTENDED USER EQUIPMENT

When on premise, unattended user assets should be secured as much as reasonably possible. Workstations should always be locked when not in use.

3.5.7.1 CLEAR DESK AND CLEAR SCREEN POLICY

1. Employees shall be required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations shall be locked when workspace is unoccupied.
3. Computer workstations shall be shut completely down at the end of the work day.
4. Any proprietary or confidential information shall be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
5. File cabinets containing proprietary or confidential information shall be kept closed and locked when not in use or when not attended.
6. Keys used for access to proprietary or confidential information shall not be left at an unattended desk.
7. Chalkboards, whiteboards, etc. shall be cleared of confidential information at the end of each meeting.
    0. Computer screens shall be set to display a password-protected screensaver after a maximum of 15 minutes of inactivity.
    1. Proprietary or confidential Information shall not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
8. Printouts containing proprietary or confidential Information shall be immediately removed from the printer.
9. For disposal, proprietary or confidential documents shall be deposited into a secure and locked container for cross cut shredding and destruction.
10. Treat Removable Electronic Media as confidential information and secure them in a locked compartment when not in use. Some examples of Removable Electronic Media are, but not limited to: CDROM, DVD R/W, USB, Portable HDD’s, etc.

4 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

5 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

6 LICENSE INFORMATION

This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode)

To further clarify the Creative Commons license related to the Open-ISM™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to Aberrant, Inc., and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the Open-ISM, you may not distribute the modified materials. Users of the Open-ISM framework are also required to refer to (http://www.aberrant.io/open-ism/license) when referring to the Open-ISM to ensure that users are employing the most up-to-date guidance. Commercial use of the Open-ISM is subject to the prior approval of Aberrant, Inc.

APPENDIX A: OFFICE FLOOR PLAN

The floor plan should be posted in the office near a location where Employees can review the document. The exits must be clearly marked on the floor plan. The location of fire extinguishers should also be plainly marked.

<<Upload an Image of your Office Floor Plan>>