Coralogix

PHYSICAL SECURITY POLICY

Version 2.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Annual Review		30/05/2020

Table of Contents

Description

This policy establishes the Enterprise Physical Security Policy, for mitigating the risks from physical security and environmental threats through the establishment of an effective physical security and environmental controls program. The physical security and environmental controls program helps Coralogix protect its Information Technology Assets from Physical and Environmental threats. Additionally, the policy provides guidance to ensure the requirements of the ISO 27001, 27701, HIPAA and PCI-DSS Security Rule are met.

Authority and Responsibility

- CISO – Ensure that employees and external factors follow the defined guidelines. Review remote access rights periodically. Ensure the effectiveness of controls implemented on access control.
- Operation Manager – defines and implements the security measures of this policy.
- IT Manager – responsible to implement all security measures deemed necessary by the CISO, internal audits recommendations and best practices. Responsible to ensure that security measures to protect equipment are in place and are appropriate.
- Coralogix Employees – should report malfunctions or cases in which equipment protection measures seem to be lacking and/or insufficient.

Definition

- PCI-DSS - The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.
- HIPAA - HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
- PHI - Protected Health Information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium.
    - ePHI - Electronic protected health information is protected health information (PHI) that is produced, saved, transferred or received in an electronic form.

Scope

- All Coralogix employees (classified, hourly, or business partners).
- All mobile devices such as laptops, smart phones, and tablets that can access, store, or transmit ePHI and/or credit card information in any way.

Method

Physical Access Control Guidelines

1. Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
2. All employee are using workstations shall consider the sensitivity of the information, including protected PII/PHI information that may be accessed and minimize the possibility of unauthorized access.
3. Access to Coralogix offices is controlled by ID cards. HR and finance file cabinets are locked when not in use. When possible, offices are locked at the end of the day.
4. Employees are responsible for their ID card access and must report any lost\stolen or broken cards to the Security Manager immediately.
5. The audit logs of the ID card access-control must be reviewed monthly to ensure card assignments are appropriate and the system is functioning appropriately.
6. The card access system must log sufficient information to produce the daily card activity reports detailed below:
    - Card identification
    - Date and time of access
    - Access attempts results
    - Unauthorized attempts
7. Updating the system access card in each change, as writhe below:
    - The date and time of the change,
    - The reasons for the change, and
    - The person who made the change.
8. Access to sensitive areas is restricted on a "need-to-work" basis.
9. The building is protected 24/7 by guards.
10. CCTV cameras and security alarms are located in Coralogix's office.
    - Both the digital recording and access-control systems must be synchronized with real time. The synchronization of the systems must be within two seconds of one another.

- All visitors must receive access in order to enter Coralogix's offices, whilst accompanied by a Coralogix employee throughout their visit. The escorting personnel must ensure that the visitors follow Coralogix's information security guidelines.

Visitor Guidelines

1. Visits to a secure area are on a need to know basis and require approval.
2. Employees who encounter an unrecognized person, who is unaccompanied, should demand that he/she identify him/herself and/or leave the offices and then notify the CISO.
3. The employee is responsible for returning the visitor's access card at the end of the visit.
4. Use a visitor logs ID card to maintain a physical audit trail of visitor information and activity, including visitor name, their company and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law. Keep the log records for a minimum of 3 months.

General Security Measures for Classified Areas

1. All personnel having access to secured areas should be aware of the enhanced information security demands of these areas, the details of the physical security perimeters of these areas, and the common responsibility for these areas.
2. An employee of a third party granted access to a secured area should be closely monitored by an escorting employee of Coralogix.
3. All parties having access to a secured area should be authorized and monitored by the CISO.
4. Empty secured areas should be kept locked and periodically checked.
5. Personnel should be aware of the existence of, or activities within, a secure area on a need to know basis.
6. Employees must maintain a clear desk and clear screen policy.

Equipment security

1. Keep access to any device that stores or processes PII/ ePHI and/or credit card information is restricted to authorized employees only. Avoid having these devices in areas that can easily be accessed by patients or visitors.
2. Ensure that PII/ePHI and/or credit card information is disposed of properly. Hard drives and any other devices that store sensitive information must be destroyed in the proper manner, and a certificate of disposal should be obtained and kept as record.
3. Keep an inventory of all devices in the office that store or process PII/ePHI and/or credit card information. Additionally, note down which employee have accesses to these devices and what roles they play in processing PII/ePHI and/or credit card information.

4. When equipment containing sensitive information is sent outside of Coralogix office for maintenance or repair controls will be activated as follows:
    - Verifying that the maintenance or repair agreement includes a declaration of confidentiality.
    - All equipment that is sent out of Coralogix's office will be recorded and documented on the equipment release form.
    - Devices must be physically secured at all times. Devices should be kept in locked offices or cabinets when not in use until he will sent out of the office.

Delivery and Loading Areas

Delivery personnel are escorted and monitored while working at Coralogix offices.

Ariel Assaraf
CEO