Coralogix

SECURITY, AWARENESS AND TRAINING POLICY AND PROCEDURES

Version 7.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		30/05/2019
2.0	BDO	Update according to ISO 27701		30/05/2020
3.0	Shiran Wolfman	Training and Awareness Monitoring Tools Metrics for training effectiveness evaluation Training and enforcement responsibilities		20/07/2021
4.0	Shiran Wolfman	Annual Review Updated competence requirement role to align with responsibilities Scope to reflect contractors		05/01/2022

		receiving training Numbering and Title adjustments		
5.0	Shiran Wolfman	Annual Review	Oded David	17/01/2023
6.0	Shiran Wolfman	Annual Review	Oded David	17/01/2024
7.0	Zach Ahrak	Annual Review	Shiran Wolfman	14/01/2025

Table of Contents

1. Purpose

The purpose of this procedure is to:

- Ensure protection of sensitive information regarding ISO 27001, 27701, HIPAA and PCI-DSS.
- Provide system and instructions.
- Assign responsibilities for identifying training needs.
- Provide the required training for establishing awareness programs. And
- Maintaining training records.

2. Application

This procedure applies to all training and awareness programs.

3. Scope

All Coralogix employees (classified, hourly, contractors, business partners).

4. Definitions

- 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.
- 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.

- PHI - Protected Health Information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or healthcare 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.

5. Procedure

5.1 General

- The objective of Coralogix training program is to ensure that employees possess the required knowledge and skills for performing their jobs; and that they are familiar with relevant requirements of the information security systems pertaining to their job functions.
- Awareness programs focus on understanding the importance of customer requirements, and the relevance of individual contributions towards meeting these requirements and achieving the security policy and objectives. Employees are made aware of the types of device defects which may occur from the improper performance of their specific jobs.

5.2 Competence requirements, security and privacy awareness and training needs

- Company-wide training and awareness programs are provided to all employees, irrespective of their function and position in the company. These programs include general orientation, rules and regulations, safety, and other such company-wide systems and issues. HR and Compliance, along with the SecOps unit and CISO are responsible

for determining requirements and identifying training and awareness needs for company-wide programs.

- Training and awareness programs will be perform when there is environmental or operational changes affect the security of electronic PHI (ePHI), credit card information or other sensitive data, for examples new or updated policies or procedures, new or upgraded software or hardware, new security technology, or new threats or vulnerabilities to ePHI and/or credit card information, and at least once a year. The training and awareness programs which perform at least once a year, will include:
    - Protection from Malicious Software - Any employee who has access to ePHI, credit card information or other sensitive data must be trained to identify the symptoms of malicious software, and the procedures for reporting and controlling such problems.
    - Log-In Monitoring - employees should be trained to recognize discrepancies in log-in procedures, and technical safeguards must be in place to detect suspicious log-in activity. Routine monitoring of account activity, such as detecting repeated incorrect password entries should be performed, and know how to recognize when their accounts may have been accessed without their knowledge. Password Management - employees should be trained in creating, changing and safeguarding secure passwords. This guidance in particular must be periodically reviewed to ensure it remains effective as password requirements change over time.
- Competence requirements and training needs for specific positions and jobs are defined in the Job Descriptions maintained by relevant departments, using Form Job Description.
- Training needs for individual employees are determined on the basis of their education, experience and job performance, including periodical evaluations conducted by Human Resources.

6. Company-wide training and awareness programs

General orientation training: Human Resources provides employee orientation training to all new and existing employees. This training familiarizes employees with administrative rules, employee programs and benefits, etc.; and explains the product, product requirements, and the information security system:

- Overview of the company's information security system;
- Discussion of security and privacy policy; and
- Explanation of how individual employees can contribute to maintaining and improving the information security system.

Participation in the employee orientation training is recorded. These records are maintained by Human Resources.

6.1 General orientation and information security system training:

- The CISO is responsible for promoting constant awareness for information security among the users of information systems.
- The Compliance Officer is responsible for issuing an awareness program at least once a year for information security which includes continuous awareness-training and updates. HR department is responsible for updating the Compliance department of incoming new employees (including their role, start date and employment emails). Compliance department is responsible for liaising with SecOps and the CISO to examine the most appropriate training courses as per certification/legal requirements and further based on the expert opinion of the CISO. Awareness for information security derives from constant exposure to security issues. The CISO is responsible for the allocation of training/marketing resources for security issues such as ePHI and/or credit card information including in the following issues:

- **Use of company-wide systems**: Wide groups of employees are trained in the use of interdepartmental systems, such as part and material coding/numbering system, bar-code system, retrieval and creation of electronic (computer) documents and records, and so forth. Training is provided by the department that is responsible for the system. Training records are maintained by the department that provides training and monitored by the Compliance Officer to ensure enforcement.
- **Media Control:** Training on media control covering removal and receipt of hardware/software including access control, accountability, data backup, data storage, mobile storage devices, and disposal of electronic data.
- **External training:** Seminars, conferences, and other forms of external training. Requests for external training are evaluated and processed by Human Resources.
- **Self-study:** The Company encourages personnel on all levels to read professional reports, magazines, and books. Requests for magazines and books are evaluated and processed by individual departments. Self-study is considered in formal recognition of skills as an alternative form of training. Where appropriate, self-study is recorded.
- **Report:** Implementing an Incident response plan that helps employees identify potential incidents, and understand what steps to follow in the event of potential data breaches.
- **Document:** Documentation of training is automated within the training monitoring tools which is supervised by the Compliance team.

6.2 Data Privacy Training:

- **DPO: Coralogix has a dedicated DPO which provides data privacy training to all employees as per GDPR article 39 (1)(b).**

- **Training is provided when the employee begins their employment and at least annually thereafter. This is implemented through the LMS as described in section 7.**

7. Training and Awareness Monitoring Tools

- **Learning Management System:** The Company uses a Learning Management System (“LMS”) to complete the required training courses online customized to the specific department and role they fulfill.
- The courses are interactive and contain questions throughout that must be passed in order to receive the certificate for the specific course.
- Emails are automatically sent to employees on their first day of employment from the LMS platform to set up their individual accounts and with a link to the required courses. Employees are required to complete critical security related courses within 1 week of the start of their employment.
- Further retraining is required on a periodic basis (yearly and quarterly depending on the role within the company).
- The LMS sends reminder emails 3 days before the completion deadline to employees who have not completed the required training.
- An email is sent to the compliance department if the deadline has passed without completion of the required training. Further action will be taken if required.

8. Departmental training

- As part of their training, personnel are made aware of device defects which may occur from the improper performance of their specific jobs. Also, personnel who perform verification and validation activities are made aware of defects and errors that they may encounter.
- On-the-job training, i.e. working under supervision of a more experienced employee, is provided to all personnel in any new or modified job affecting product quality. On the-job training is recorded, to include its scope, duration, and the name of the person who supervised the training.
- Employees who have been performing their jobs or functions for at least six months prior to the initial implementation of this procedure may have their qualifications

formally confirmed by their supervisors or departmental managers, without having to go through the initial training. This confirmation is documented in a written statement, including specific designation of the particular jobs and functions for which the employee is being confirmed. The confirmation record is equivalent to a training record, and is filed and maintained as such by Human Resources.

- Employees who do not perform satisfactorily are provided with additional or repeated training.

9. Training effectiveness evaluation

The method used for evaluation of effectiveness for each training activity will be proportionate to the risk involved in the work for which the training is provided. The following methods and approaches are used for evaluating the effectiveness of training provided:

- Follow-up evaluation of individual employees: Following competency or skill training, employees are evaluated by their supervisors or departmental managers. This evaluation assesses whether a particular training has achieved its objectives and if the employee is sufficiently competent and/or skilled to perform the new job function for which he or she was trained. Results of this evaluation are recorded and are kept together with the original training record.
- Review of overall performance in areas related to particular training: When wider groups of employees are trained in safety, emergency procedures, or interdepartmental systems, this type of training is evaluated by comparing statistical performance data from before and after the training was provided. For example, the effectiveness of safety training is measured by tracking rates of work-related accidents.
- Correlation of training with nonconformists and system failures: Training and competency are always considered when investigating causes of product and process nonconformities and failures of the information security system. When inadequate training is the cause, the investigation goes further to determine specifically which particular training is at fault. This training is then reviewed and improved, by changing its scope, format, or frequency, as appropriate.

- Global evaluation of training by management review: Training and awareness programs and their effectiveness are evaluated by management reviews. This includes presentation and discussion of data correlating information security performance in particular areas with specific training and awareness programs. Operational Procedure Coralogix, Management Review, defines this process.
- LMS metrics: Employees must complete testing during the process of completing required courses within the LMS. Metrics are predefined to evaluate employee understanding of materials and to ensure an adequate level of comprehension based on the risk associated with each topic.