Coralogix

INFORMATION SECURITY POLICY

Version 9.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Annual Review		30/05/2020
3.0	Shiran Wolfman	Training and Awareness Monitoring Tools		20/07/2021
4.0	Shiran Wolfman	Policy Maintenance		18/09/2021
5.0	Shiran Wolfman	Vulnerabilities Management and Sources		18/10/2021
6.0	Shiran Wolfman	Annual Review		18/01/2022
7.0	Shiran Wolfman	Annual Review	Oded David	17/01/2023
8.0	Shiran Wolfman	Annual Review	Oded David	17/01/2024
9.0	Shiran Wolfman	Updated vulnerability sources- internal pen tests as source and clarified external pen test timelines	Oded David	13/08/2024

Table of Contents

1.0 Executive Summary

Coralogix helps software companies to map their software flows, automatically detect production problems and deliver pinpoint insight.

Coralogix comply with security laws, regulations and standards including ISO 27001, 27701, HIPAA and PCI DSS.

This policy sets forth the framework for Coralogix's compliance with the Security Rule of ISO 27001, 27701, HIPAA and PCI DSS.

Coralogix does not directly hold customers PII/ePHI and/or credit card information. This information can be kept by user's activities logs.

The intention with this policy is to align Coralogix with all relevant requirements with regards to system and data management, including laws, regulations, agreements, Service Level Agreements, Operating Level Agreements and good business practice.

Coralogix accepts credit cards as payment for a variety of services. By accepting credit cards, Coralogix assumes significant risks with respect to protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed a set of financial and information technology standards, called Payment Card Information Data Security Standards (PCI-DSS), to protect credit cardholders’ data.

The company will ensure the portability of health insurance benefits particularly as individuals moved from job to job.

The considerations for dealing with information must, as a minimum, include Information Lifecycle Management considerations spanning all media on which the information is stored or transits as well as procedures for managing access rights.

The Chief information security officer (CISO) is empowered to jointly take decisions regarding Information Security.

2.0 Empowerment

Decision power is granted to CISO over all matters relating to Information Security. Areas covered by other functions must be decided in conjunction with the relevant parties. That is the case for, for example, Legal issues (Legal Department).

3.0 Laws and Regulations

Coralogix undertakes to comply with the laws and regulations governing the processing of personal data where Coralogix operates, including, but not limited to, the ISO 27001, 27701, HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS (Payment Card Industry Data Security Standard), the GDPR (General Data Protection Regulation), SOC2, etc.

These laws and regulations have an impact on data management, for example data retention of employee data and more. Legal Department is responsible for the identification of new relevant laws and changes to existing laws. The CISO monitors the evolution of technology currently in use by Coralogix as well as of information security risks.

4.0 Principles

The policy defines the standards, which require covered entities to implement basic safeguards to protect the confidentiality, integrity, and availability of PII, electronic protected health information (ePHI) and/or credit card numbers and transactions information. Privacy depends upon security measures: no security, no privacy.

In accordance with the laws and regulations governing the protection of personal data, the core principle of the ISP (Information Security Policy) is that data managed by Coralogix is managed securely, meaning that the CIA (Confidentiality, Integrity and Availability) of the information is ensured at all steps in its lifecycle or, in other words, Information Lifecycle Management considerations must be applied and working procedures must take all the steps reception,

creation, usage, sharing, transmission, storage, backup, archiving and destruction of data into account.

1. Coralogix Management is committed to the information security program. The management will provide the necessary resources to sustain the program including people, tools, processes, procedures, and education.

2. Coralogix will maintain an inventory of all its information assets, regardless of its physical and geographical location. All assets will be classified, to ensure that all information receives an appropriate level of protection, including encryption and hardening when required.

3. Coralogix's Information Security plan will be driven by an ongoing assessment of the risks posting its information assets.

4. Coralogix will ensure that employees, contractors, partners, and vendors understand their security responsibilities.

5. Coralogix will ensure that only authorized users will have access to its information assets and services.

6. Coralogix will ensure that information security will be designed and implemented within the whole development lifecycle of its products.

7. Coralogix will identify compliance requirements, including contractual, regulatory and legal requirements, and integrate them into the Information Security Program as necessary.

8. Coralogix will ensure that every single employee works to prevent information security incidents from occurring. Should an incident take place, we will swiftly implement appropriate actions, including those preventing recurrence.

9. Coralogix will ensure that its partners, suppliers, and contractors will maintain adequate security measurements to secure of Coralogix's and its customer's information.

10. Coralogix will ensure continual improvement of the Information Security Management System (ISMS) and Privacy Imformation Management System (PIMS).

11. Comply with methods from international laws, regulations and standards for information security, e.g. ISO 27001, 27701, HIPAA and PCI DSS.

4.1 CIA Confidentiality

Confidentiality means that data should be accessible only to those who need access to that data and that it should be possible to identify who made data changes; for a reasonable period of time.

4.2 Integrity

Integrity means that

1. Data shall be protected from unauthorized alteration;
2. It shall be possible to trace who or what changed a dataset (e.g. logs, tracing tables)
3. Application level data integrity controls shall be taken into account (e.g. control totals, automated reconciliations)
4. Data automatically shall be protected (either prevented or detected and corrected) from system failures and catastrophic events, wherever possible and reasonable.
5. Persistent storage shall be considered (e.g. duplication / redundancy, backups)

4.3 Availability

Availability means that the risk of system availability and data loss should be taken into account when designing a system making sure that business requirements are met. It is expected that availability requirements are defined based on customer expectations and a business impact analysis.

5.0 Purpose and Scope

1. This policy establishes Coralogix's commitment to manage the risks affecting the confidentiality, integrity, and availability of information within the organization, business partners, and subsidiaries.

2. The Information Security and Privacy Program is an essential component of the strategy to protect Coralogix's reputation and corporate image.

3. This policy serves as the foundation for detailed security documentation such as guidelines, standards, processes, and procedures based on the principles outlined below.

4. Coralogix is committed to protect its PII/PHI, credit cards information and that of its customers. To achieve this goal, the company has implemented ISO 27001, 27701, HIPAA and PCI DSS controls and commit to comply with them.

6.0 Dimensions

Digital information generally transits the following elements:

1. Network (routers, switches, firewalls, proxies, etc.) Systems

2. Applications Databases File servers (recipient for unstructured information) Portable media (usb keys, dvds, paper, tape ...)

3. And it is expected that the security and availability aspects of these areas are managed, meaning taking CIA into account on each of these levels. The general principle regarding security is "need-to-do, need-to-know". Availability criteria should be based on sound risk management principles.

7. Risk Assessments

Coralogix will perform a yearly risk analysis, which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of PII/ePHI managed by the covered component. Departments which accept credit cards may be subject to a risk assessment.

In accordance with risk analysis, the company will implement measures to reduce computer risks and vulnerabilities, including identifying and documenting potential risks and vulnerabilities that could impact systems processing PII/ePHI; performing annual technical security assessments of systems processing PII/ePHI in order to identify and remedy detected security vulnerabilities.

Risk assessments are expected to cover, over time, all the relevant dimensions:

External access (firewalls, routers, web applications,...) **Internal access** (logical security, change management, ...) Data integrity (configuration management, storage control, processing error control ...) System and data availability (redundancy, monitoring, incident management, ...) Service delivery (customer reporting, financial control, policy & process adherence, ...)

All employees involved in processing credit card payments and PII/PHI information must be aware of this policy, understand the risks associated with their handling of sensitive information, and complete security training related to handling of cardholder data and health information.

Vulnerabilities Management

Coralogix identifies vulnerabilities through a vulnerabilities assessment process identified in its Risk Assessment Methodology. Vulnerability reports are collaborated on with the CISO and security team and enforced by Compliance through confluence vulnerabilities management page, where remediation work is prioritized (through a risk calculator) and tracked. Critical vulnerabilities are reported to management and executives and granted top priority to issue and

deploy a fix. Other vulnerabilities are prioritized and fixed per development scheduling period, and through vulnerabilities patch management collaboration.

Vulnerabilities Sources

Vulnerabilities are identified through several sources and are labeled, tracked and assessed. External internal penetration tests are conducted on a semi-annual basis by authorized expert 3rd party assessors, including re-tests to verify remediation of vulnerabilities within industry standard SLA's. Internal penetration tests are conducted by our security researchers with a defined scope and under the guidance of the Coralogix CISO. Network vulnerability scans are conducted regularly. Various other scanning tools are used to cover the entire depth of our systems and lifecycles. A bug-bounty program is established and available to external security researchers.

8. Data Protection Impact Assessments

Coralogix will, when acting as the customer's processor within the meaning of ISO 27001, 27701, HIPAA and PCI DSS, assists the customer in carrying out Data Protection Impact Assessments related to data protection.

9. User Access Management

A lot of customers' transaction data provided to Coralogix as part of day to day operations is subject to data privacy laws. In that respect, it is expected that physical and logical access controls are developed with the "need to do, need to know" principle in mind.

Access shall be managed on all the levels mentioned in section Dimensions. It is required to maintain system access logs. It is recommended to have activity logs and have these centralized and monitored for suspicious activity. Access will be reviewed periodically.

The process of granting and revoking normal user access shall in general be initiated by HR, implemented by IT, where possible be based on roles, groups or profiles and reviewed at least yearly.

Requirements and expectations with regards to end-users are covered in the “Coralogix User Access Management”.

10. Security and Privacy Awareness and Training

An important aspect of user access management is that the users are aware of their basic obligations. To meet that requirement, it is expected that newcomers in particular are given a security awareness training, at least in the beginning of their employment.

Security awareness training will include instructions about the use of PII/ePHI and credit card information. Additionally, security policies and procedures must be published centrally and kept up to date at all times.

11. Training and Awareness Monitoring Tools

Learning Management Software: The Company uses a Learning Management Software (“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.

12. Physical Security

To protect the critical assets from theft, vandalism, destruction by error, or any other data breach, machinery used for service delivery purposes should be kept a secure manner; access to which should be limited to relevant personnel. Access to office spaces should also be restricted, for example by swipe cards.

13. Business Continuity and Disaster Recovery

Coralogix's have procedures in place to respond to an emergency or other occurrence that damages systems processing PII/ePHI and credit cards information.

The company measures that all PII/ePHI and credit card information will address include having procedures for creating and maintaining backups adequate to both restore and the systems maintaining this data.

In addition to the timeliness of the service delivery, other factors like penalties, lost revenue, customer satisfaction (renewal impact ...) should be taken into account.

14. Data Classification and Data Protection

Coralogix recognizes several classes of data and distinguishes their treatment accordingly. Generally, data shall be protected from

unauthorized alteration, accidental or willful loss, and any data breach and other prohibited or unauthorized data transfer in all dimensions under the control of Coralogix.

To prevent loss, it is expected that mission critical data, including customer data, is copied, duplicated and/or backed up to a different geographical location than where the original (to Coralogix) is stored.

To prevent data breach, technical and organizational measures have been adopted, it is expected that personal data, including employees and customer data, is compartmentalized and secured by appropriate and confidential means of access to which only authorized persons have access.

15. Incident Management

Anyone may report cases of suspected fraud or abuse. All employees are required to report any actual incidence of theft or fraud. If you believe that an incident has occurred, please notify the CISO immediately.

Coralogix have procedures in place to handle security incidents, including incidents that involve PII/ePHI and credit card information. Employees are aware to notify the CISO when a system processing PII/ePHI and/or credit card information is involved in a security incident (examples include virus or worm infection, accounts being compromised, and servers damaged from a denial of service attack).

16. Policy maintenance

1. Coralogix will maintain the policy document and information security procedures:
    a. The policy document will be valid and update every year, under the responsibility of the CISO. Maintenance of policies and procedures, including any changes, will go back at least 6 years in line with HIPAA policies, procedures and documentation requirements.
    b. The information security policy will be approved by the Management of Coralogix and will be published to all company employees.
2. Coralogix will take the following actions to endure the implementation of the policy:
    a. Conducting tests to expose vulnerabilities and weaknesses in information security.
    b. Conducting security reviews (information security risks and/or penetration tests) once a year, analyzing the findings and determining work plans for handling the findings.
3. Every employee with access to PII/ePHI is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to $250,000 per year and criminal sanctions including fines and imprisonment.
4. Compliance with the PCI-DSS requirements shall be enforced by the CISO. The CISO is responsible for risk assessments, vendor review and periodic scanning for sensitive information. Additionally, the CISO is the authorizing entity for the quarterly compliance statements required by PCI-DSS.