Coralogix

HUMAN RESOURCES SECURITY POLICY

Version 5.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Shiran Wolfman	Initial Version		06/09/2021
2.0	Shiran Wolfman	Applicant Tracking System: process and enforcement		15/11/2021
3.0	Shiran Wolfman	Annual Review		18/01/2022
4.0	Shiran Wolfman	Annual Review	Oded David	17/01/2023
5.0	Shiran Wolfman	Annual Review	Oded David	17/01/2024

Table of Contents

1.0 Purpose

The procedures of this policy are split into 3 key stages of a user's access to information or information systems used to deliver Coralogix's business.

1. Prior to employment- to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. checks must be made to ensure that the individual is suitable for access to Coralogix information systems.

2. During employment- to ensure that employees and contractors are aware of and fulfil their information security responsibilities. Their access must be regularly reviewed to ensure it remains appropriate.

3. End of employment/role change- when a user's requirement for access to information or information systems ends (i.e. when a user terminates their employment with Coralogix, or changes their role so that access is no longer required); access needs to be removed in a controlled manner.

This policy also addresses third party access to Coralogix information systems (e.g. contractors, service providers and partners).

2.0 Scope

The policy applies automatically to all employees of Coralogix, including contractual third parties that have access to Coralogix information systems (including components and physical systems/tools).

To reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Coralogix information systems must:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after access to information systems.

Access to Coralogix information systems will not be permitted until the requirements of this policy have been met.

3.0 Laws and Regulations

Guidance	Section
ISO 27001: 2013	A.7 (A.7.1, A.7.2, A.7.3)
HIPAA	164.308(a)(1)(i), 164.308(a)(5)(i) 164.308(a)(6)(i), 164.310(a)(1)

4.0 Policy Governance

The following table identifies who within Coralogix is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of Human Resources
Accountable	Compliance, CISO, Management
Consulted	Security team
Informed	All employees, contractors, relevant third parties

4.1 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Compliance at least annually or when a significant change occurs.

5.0 Prior to Employment

All candidates for employment, including contractors, must undergo background verification checks in accordance with the appropriate laws. The screening must include verification of:

o Identity

o Education, skills and experience

o Employment history

o Character references

- A criminal record check will be conducted (in jurisdictions where it is permissible).
- Contractual agreements with all employees and contractors will clearly outline the responsibility of the individual/contractor to information security. The terms and conditions for contractors and external party users must include:
  o A confidentiality or non-disclosure agreement

- o Legal Responsibilities and Rights
- o Responsibilities for the classification of information and management of assets
- o Responsibilities for the handling of personal information

5.1 Applicant Tracking System

As part of the pre-employment phase Coralogix uses an ATS in order to organize and filter out prospective applicants based on pre-defined criteria. These criterias include; required skills and prior experience. Coralogix uses Comeet as our primary ATS in order to ensure collaboration and transparency amongst relevant stakeholders during the recruitment process.

Enforcement:

The ATS ensures Coralogix's defined procedure is followed and enforced in regards to the interview process up to and including required background checks. The procedure is mapped out visually in the platform; tracked by the head of HR and enforced by Compliance.

6.0 During Employment

CISO must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their work, and to reduce the risk of human error. It is also necessary that employee/contractor changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

Management must notify the appropriate function in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate.

Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to user access must be made in a timely manner and be clearly communicated to the user.

Management must require employees/contractors to understand and be aware of information security threats and their responsibilities in applying appropriate Coralogix policies. These policies include:

- Information Security Policy.
- Physical Security Policy.
- User Access Management Policy.

All Employees/Contractors receive appropriate information security awareness training and regular updates in related organisational policies and procedures as relevant for their role.

It is the role of management to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely. It is the role of the Compliance department to enforce management compliance with these obligations.

7. End of Employment/ Role Changes

Managers must advise personnel of their information security responsibilities when employment changes or is terminated. Terminated employees and contractors must be made aware of:

o Ongoing security requirements including the need to not disclose sensitive information.

o Responsibilities described in confidentiality or non-disclosure agreements (including non-compete obligation).

o Any other applicable policy standards or contract.

o This process includes exit interviews and removal of documents in any format (and all copies thereof) and other Coralogix property and materials in their possession or control.

Processes are implemented to ensure that all access rights of users of Coralogix information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Processes are implemented to ensure that all hardware is immediately returned and wiped of all sensitive data. This process is catalogued and documented by the security team.

Processes and responsibilities are implemented to enable emergency suspension of a user's access when that access is considered a risk to Coralogix or its systems as defined in the Information Security Policy and User Access Management Policy.

8. Non-Compliance

In cases where it is determined that a breach or violation of Coralogix policies or procedures has occurred, management will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors or third parties the termination of a contract or agreement.