Coralogix

USER ACCESS MANAGEMENT

Version 2.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Update according to ISO 27701		30/05/2020

Table of Contents

Description

- Formal procedures should be in place to control the allocation of user access rights to information systems and services.

- The procedures should cover all stages in the life cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services.
- Special attention should be given, where appropriate, to the need to control access to production and the allocation of privileged access rights, which allow users to override system controls.
- This procedure relates to information in files, servers and workstations, software and databases.
- Information owners should allow access to systems on a "need to know"; basis, according to the job requirements of the user.
- Access rights granted to users should not contradict the principle of separation of duties.

Scope

- All Coralogix employees (classified, hourly, or business partners).
- All type of access to workstations, programs and other processes that may display, contain or process PII/ePHI and/or credit card information.

Terms and 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 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.
- **Access to production:** Logical or physical access to Coralogix's production or MIS environments (e.g. servers containing applications, databases with users information etc.)
- **Classified/Sensitive Information:** Any information pertaining to the privacy of the individual or to the Company's business.

- **Termination of employment:** this definition may be instituted on an individual that is terminated or resigns from his post.

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.
- **The IT Manager -** Ensure that access rights to the network (locally and remotely), Production accounts and attribution to distribution groups (e-mail) are given in a formal and documented manner according to this procedure.

General

When allocating access rights to various factors according to ISO 27001, 27701, HIPAA and PCI-DSS the following guidelines will be up held:

1. For high level authentication techniques users will be assigned Multi Factor Authentication (MFA), which require them to enter two of the three security "factor":
    - "Knowledge" factor: Password or Pin.
    - "Possession" factor: Something you have.
    - "Inherence" factor: Something you are.
    - "Location" factor: Somewhere you are.
2. MFA require from all users who linked to their activities and be held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons.
    - Each user will be granted access rights according to his affiliation to a specific group, and according to the “need to know” principle that includes access both to the data itself, as well as to the systems that store, process and transmit that data. The level of access granted is appropriate to the business purpose, and is consistent with organizational security policy, e.g. it does not compromise segregation of duties.
    - Granting of access rights and access privileges will be carried out according to this procedure – i.e. the process will involve a chain of approvals and will be documented all establishes the identity of the user and the need to access the ePHI and/or credit card information and reviewed.
    - Access rights to Coralogix network (locally and remotely) and association to a distribution group will be granted by the IT Manager.

- Access to the production environment will be approved only on a "must-have" basis granted and implemented by the VP of R&D.
- When a user needs access to production information, he will present a justified business argument in order to access the data and gain permit from their owner.
- The IT department will modify user access rights to ensure that the appropriate level of access is granted at all times and will ensure the protection of any new file or operating system component to prevent inappropriate, general access.

User Registration

User registration to Coralogix's network will be done as follows:

1. Upon arrival of a new employee, the HR department will inform the IT Manager of a new employee. The direct manager of the new employee will request, via email, to the HR Manager and the IT team, to open a new user account and provide them with the necessary access rights. The IT team may open a new account for the employee based on HR's notification, however, in order to provide additional access rights to shares or additional access to production, the VP R&D must be provided in an email from the direct manager of the new hire.
2. HR Manager and IT Manager will ensure that all new employees are trained during their orientation, to include information on the degree of access permissible by their job functions, security policies and procedures, and setting of passwords.
3. In cases where the access rights should be given for a limited period (e.g. for the duration of a project), the time period must be stated in the request. The direct manager will inform the IT team and/or the VP R&D whenever these privileges are no longer required.
4. In cases in which the privileges are not approved, a notification will be forwarded to the direct manager.
5. The IT team will then forward details of user account and password (to network and to other relevant systems) to new employees.
6. The employee will change password upon first logon (see paragraph 8 for password policy details).

Revoking System Access

Whenever a user terminates his employment in the company, the following will be done:

1. HR or the direct manager will immediately inform the IT Manager in order to have all of the employees'; privileges revoked (especially in cases where an employee is terminated due to reliability reasons or information security breaches).
2. Access rights of employees on long leaves will be disabled so as not to be of use to other employees. When the employee will return from the leave of absence, the direct manager will inform the IT team of his / her return via e-mail. The IT Manager will activate the account and document the e-mail correspondence for future reference.
3. Default accounts defined by vendors of the different systems (Guest, Anonymous), must be removed or neutralized.
4. User accounts will be locked, after 5 aborted access attempts to any system.
5. Restrictions on connection from specific workstations to specific systems will be applied when required.

User Password Management

Password Management

1. Users are required to keep personal passwords confidential and keep group passwords solely within the membership of the group.
2. Passwords will not be stored next to workstations or in plain sight.
3. Username and passwords are personal and may not be transferred to another. Every employee will be held accountable for his / her actions.
4. When a user forgets his/her password, they may request password reset from the IT manager after clearly identifying himself.
5. The temporary password will be confidentially given to the user. The password will not be given by a third party or by an unprotected text in Email. The users will acknowledge receipt of password.
6. Password will not be stored in computer systems in an unprotected manner.

Password Rules and Defaults

1. Each user will have a unique ID.
2. Password length will be 8 characters at least, composed of letters, numbers and other special signs.
3. The default password will be changed in first log on to software\system.
4. It is forbidden to create fixed passwords that could be related easily to the organization or to the user (e.g. names, birthdays etc.).
5. Operating system will impose change of temporary passwords at first logon.
6. Users will be required to change passwords to Coralogix's network every 90 days, and network system will keep history of 10 recent passwords.
7. User account will be locked out after 5 failed log-in attempts.

User Access Rights Survey

1. Removal of default access and passwords - default accounts defined by vendors of the different systems (Guest, Anonymous), must be removed, disabled or have the password changed from the default value.
2. Reassessment of access rights – IT Manager together with information owners are responsible to perform a periodic survey as to user access rights to owned information assets (shares / folders / files / systems / environments etc.) every 6 months.
3. The CISO will perform a bi-annual access rights survey with the assistance of the IT manager.
4. The survey will include:
    - An examination that no dormant accounts are in place (in accordance to HR termination list and / or last logon logs).
    - Access rights are allocated in accordance to business needs, i.e. there are no excessive access rights.
    - Access rights process management is documented (review new / changed and deleted accounts in accordance to the manager's email request).
    - Access to PII/PHI information.
5. Excessive user rights will be revoked.
6. Findings of this survey will be reported to the Information Security Steering Committee and additional management members when necessary.
7. Review of access rights to the cloud environment will be performed by the cloud manager twice a year.

Ariel Assaraf

CEO