CODE OF CONDUCT REGARDING PRIVACY & DATA PROTECTION

Summary

The code of conduct describes a set of information security principles, applicable to all employees, internal and external.

Principles

Reporting incidents

You have the responsibility to report a (suspected) information security incident as soon as possible to the security officer, following the Incident management process.

1. Password handling

1.1 Technical conditions

When setting a new password it is important that the following requirements are met:

- Passwords must be at least 8 characters long
- Passwords must contain uppercase, lowercase, letters, a special character and at least 1 number.
- The passwords must be changed after 180 days where possible (Auto expire)
- New passwords may not be similar to the last 3.
- When an account is created the user will be forced to change the password after first sign on.
- The usage of biometrics is allowed and encouraged within the company.
- The usage of a password managers like KeePass or 1Password is encouraged

MFA is enabled on all accounts and you can view the complete password policy as created by our IT service provider on CTOUCH Sharepoint.

1.2 Account sharing

It is not allowed to share passwords or accounts with other people within or outside of the company.

- The employee is responsible for changing the password if he/she suspects that someone else is using his/her account. They must also report this to our IT service provider.

2. Clean desk policy

- The employee must ensure that there are no confidential data or passwords left unattended.
- Sessions must always be locked or logged off when you leave your desk.
- Key cards, credit cards/debit cards or keys may not be left unsupervised (If left at a drawer make sure that it is locked.)
- When printing Confidential or Sensitive information the employee must immediately pick them up from the printer.
- Do not leave your notebook or phone in plain sight at the office after working hours (see Endpoint Device Policy for more information).

3. Usage of meeting rooms

- The employee must ensure that there are no confidential data or documents left unattended in the meeting rooms.
- If the whiteboard in the meeting room is used the employee must ensure that the whiteboard is cleared and that there is no confidential data stored.

4. Usage of internet & remote working

4.1 Employees

When an employee wants to work remotely or access the internet from inside our outside of the company network he will need to make sure that the following criteria are met.

- If the employee wants to access the internet from outside of the company network they will need to either use a VPN or hotspot. The usage of open (unprotected) networks is prohibited.
- It is not allowed to access websites or content with company owned devices or on the company network which could contain viruses.
    - This includes websites with adult or gambling content for example.
- It is not allowed to download and install applications from unknown sources.
- The end user must when in doubt of spoofing/phishing/spam activity contact the IT service provider (Link-IT).
    - If further action is required Link-IT will contact the security officer.

4.2 Guests

- Laptops of guests may only be connected to the wireless guest network.
- Guests are not allowed to access illegal websites from within the guest network.
- Guests are not allowed to connect their devices via an ethernet cable.

5. Endpoint device policy

- The device must be enrolled in Microsoft Intune
- The disk must be encrypted via BitLocker
- The device must be protected using a password, pincode or biometrics.
- The below policies are only applicable for company owned devices.
    - Remote device wipe is enabled.
    - Remote device is enabled.
    - Locate lost or stolen device is possible.
- The device must lock and prompt the user for a pincode/password after a specified amount of time (5 min).
- Applications may not be installed from an unknown source (contact the security officer when you are in doubt).
- Access to physical USB ports must be disabled were possible. If you want to use a USB drive contact the security officer to see what is possible.

6. Usage of e-mail

- Employees may occasionally and briefly use the e-mail system to receive and send personal e-mail messages, provided it does not interfere with daily work and the company network.

    - Sending e-mail messages must meet the following conditions:
        - All incoming mail traffic must be scanned.
        - Suspicious mail attachments like .html for example must be blocked.
        - When sending confidential information via mail encryption in Outlook must be used.
        - The end user must when in doubt of spoofing/phishing/spam activity contact the IT service provider (Link-IT).
            - If further action is required Link-IT will contact the security officer.
        - The sending of attachments (with a bigger file size) should be limited as much as possible in business e-mails.
            - The sending of attachments is not allowed in private e-mails.
        - GDPR sensitive information may never be shared by mail. The end user may only verify said information, but not actively share it.

7. Acceptable use of Internet and social media

- You are free to use Internet for private matters, within reasonable limits and as long as it does not violate any laws or company policies.
- You are allowed to use social media, if you realize you are speaking on behalf of our organization.
- Usage of WhatsApp is allowed and WeChat is only allowed to communicate with certain suppliers as long as it does not violate any laws or company policies.
    - Access to WeChat must be requested via the department manager.

8. Logging

- Monitoring is done by MMOX and Fortianalyzer.
    - Traffic is monitored actively and unusual activities are reported to the security officer within the company.
    - CTOUCH receives monthly reports and these are analyzed and active vulnerabilities are patched/resolved.
    - The lead software developer actively monitors websites like exploit-db and makes sure that the developed software is not vulnerable.
        - The security officer will receive a list with patched vulnerabilities from the lead software developer.

9. Physical security

- Loss of a mobile device or laptop must always be reported to the IT service provider (Link-IT). This is also the case when the device is lost after working hours, during a holiday or in the weekend.
    - Link-IT will take further actions like remotely wiping the device to make sure that no confidential data falls in the wrong hands and inform the security officer.
- Loss of key card or keys which could grant access to the company should always be reported to the manager.
- Malfunctioning security measure (such as a lock or alarm);
- Not locking the doors/windows or not enabling the alarm after working hours;
- Malfunctioning hardware or software;
- Data leak or breach of confidentiality;
- Breach of policies or guidelines;
- Access violations. (Also includes physical or unauthorized access)
- Suspicious activity like spam or fishing mail

- At a later stage, it will no longer be possible to authenticate as a guest via a LAN cable.

10. Data sharing

10.1 USB

- It is not allowed to share confidential data via USB.
- A user is not allowed to connect unknown USB devices to company owned device.
- The usage of USB drives is by default not allowed unless this is absolutely needed to perform daily work activities.
    - In case the user needs a USB drive to perform daily activities he will need to ask his manager for permission.
      The manager will check if this is needed and create a ticket with Link-IT when access is granted.
        - Link-IT will contact the security officer when in doubt.

10.2 Bigger files

- Confidential data may only be shared via OneDrive.
- Non-confidential data may also be shared via WeTransfer.

11. Disciplinary measures

We have an open culture in which it is not bad to make mistakes. It is however important that we learn from these mistakes and that it gets reported in a timely fashion. Should it be necessary to take action, this is at the discretion of the management. They will take care of this.

If this code of conduct is violated, measures may be taken depending on the nature and seriousness of the violation. These include disciplinary and employment law measures. They may include deprivation of the right to use the Internet, an official warning, transfer, suspension, termination of the employment contract and reporting to the police.

CTOUCH reserves at all times the right to investigate accounts and assets.

12. Requesting rights and changing roles

During the onboarding and changing of roles you receive the access rights and roles you need to fulfill your duties. However, it might occur that you need to gain more access rights to be able to perform a task. It is possible to request more rights with the information system owner. The request will be logged by creating a ticket "Aanvragen rollen en rechten". It should contain which account should get additional access rights, which rights are needed and why they are needed. If accepted the access rights will be granted. Otherwise the information system owner will explain why the request was denied

13. Receiving guests

ALL visitors to CTOUCH must be registered in the cu@ctouch.eu agenda. In this way we can:

- Get a clear overview who the expected visitors are,
    - so that we are not surprised when the bell rings
    - we leave a professional impression to the visitor
- Easily find who has visited our office and when and at what time/for how long.
- Inform the BHV-organization in case of an emergency

Visitors are only allowed to visit if they are guided by a host. The host is a CTOUCH-employee. Visitors are always accompanied under the responsibility of the host.