Purpose

The purpose is to protect data understood as:

- Personal data

- Sensitive data

- Confidential information of customers, contractors and employees.

All employees and associates who have access to the data **are responsible for the implementation of the policy**.

Data Processor:

- ensure that a clean desk policy is in place,

- take care of the security of documents containing data,

- supervise documents during the absence of another employee, if they have taken over their supervision,

- inform the direct supervisor about the lack of application of the procedure,

- inform the person responsible for data security about incidents.

If an employee leaves the workplace, even for a short time, they should:

- transfer the paper documentation containing the data to your locker and lock it with you and take the key with you.

- Turn off/log off the workstation and make sure that no data media is left unprotected.
    - Make sure that your workstation has an automatic screen saver set to block access to data.
    - Make sure that you can resume work only after you enter your password.

Important documents should be sent by registered mail with acknowledgment of receipt or use the services of trusted courier entities, choosing, if possible, the service with personal delivery.

It is forbidden to receive guests in rooms where data is or may be processed.

In exceptional circumstances (e.g. ongoing maintenance work), access to the premises of a person who is not authorised to process data is allowed. This is done in the presence of an employee with appropriate authorizations. Before bringing such a person into the room where the data is processed,

it should be ensured that it is not possible for him or her to inspect the documents containing the data.

When using shared printing devices, it is not allowed to leave the machine unattended during printing/scanning/copying if the materials in the machine contain data.

End of work shift:

- Leave the desk clean
- any paper document containing data drawn up as a working document must be secured or destroyed

After the end of work, third parties may appear in the rooms, e.g. building security, cleaning service or technicians – they should also not have access to the data.

Clean desk principle:

- When you're done, put all the documents on your desk in a safe place.
- Do not leave the closet key in the lock.
- Do not write down passwords on sticky notes that you stick to your monitor or in any electronic form except password managers.
- Print important and confidential documents only when supervised, and take them right away from the printer.
- Shred documents containing data in a shredder or dedicated containers, the contents of which are shredded by an external company.
- Erase whiteboard notes as soon as the meeting ends.
- If you're leaving your computer, lock it or start the screen saver.
- If you leave the office without a laptop, put it in the locker.
- Do not drink or eat at the computer.
- Protect data carriers (external drives, flash drives, phones, tablets) from unauthorized access.
- Do not store unnecessary/unused data on the desktop, local drives, "Download" folder outside of the qualified systems/resources listed in the Processing Activities Record QI 44.