**Techmojo ISMS CLEAR DESK POLICY**

Diagram

Description automatically generated

Use of locked areas: lockable drawers, archive cabinets, safes, and file rooms should be available to store information media (e.g., paper documents, USB flash drives, memory cards, etc.) or easily transportable devices (e.g., cell phones, tablets, and notebooks) when not required, or when there is no one to take care of them. Beyond the protection against unauthorized access, this measure can also protect information and assets against disasters such as a fire, earthquake, flood, or explosion.

Protection of devices and information systems: computers and similar devices should be positioned in such a way as to avoid people passing by to have a chance to look at their screens, and configured to use time-activated screen savers and password protection to minimize chances that someone takes advantage of unattended equipment. Additionally, information systems should be logged off when not in use. At the end of the day the devices should be shut down, especially those network-connected (the less time a device is on, the less time there is for someone to try to access it).

Restriction on use of copy and printing technology: the use of printers, photocopiers, scanners, and cameras, for example, should be controlled, by reducing their quantity (the fewer units available, the fewer potential data leak points) or by the use of code functions that allow only authorized persons to have access to material sent to them. And, any information sent to printers should be retrieved as soon as practicable.

Adoption of a paperless culture: documents should not be printed unnecessarily, and sticky notes should not be left on monitors or under keyboards. Remember, even little pieces of information may be sufficient for wrongdoers to discover aspects of your life, or of the organizations’ processes, that can help them to compromise information.

Disposal of information remaining in meeting rooms: all information on white boards should be erased and all pieces of papers used during a meeting should be subject to proper disposal (e.g., by using a shredder).

How to implement a clear desk and clear screen policy

According to ISO 27001, control 11.2.9, the main orientation is to adopt a Clear Desk and Clear Screen Policy considering:

the level of information (e.g., sensitive or confidential) that would require secure handling

legal and contractual requirements that demand information protection

identified organizational risks

cultural aspects

measures that should be adopted to secure desks, devices, and media (as seen in the previous section)

Besides that, an organization also should consider periodic training and awareness events to communicate to the employees and other people involved the aspects of the policy. Good examples are posters, email alerts, newsletters, etc.

And, finally, there should be periodic evaluations about the employees’ compliance with the policy practices (let’s say, two times a year).

Do not be victim of prying eyes and unauthorized access

A lack of care with a workspace can lead to compromised personal or organizational information. Passwords, financial data, and sensitive emails can be disclosed, impacting privacy or a competitive edge. A lost document containing information about a contract/proposal due date can cause a tender to be lost and a decrease in the expected revenue.

Whether due to accidents, human error, or malicious actions, these negative results can be avoided by the adoption of accessible low-tech measures related to a clear desk and clear screen policy. So, do not wait for these situations to occur before taking action. In this case, the solution’s cost would hardly be an excuse to not act preventively.