Clear Desk and Clear Screen Policy

Objective

Interr Ltd is committed to preserving the confidentiality, integrity and availability of its data. This policy will help ensure that all sensitive/confidential materials is kept secured at all times. The policy will help reduce the risk of security breaches within the workplace. Its intent is to protect information stored in physical and electronic media and minimize the risk of unauthorized access.

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, agents, contractors, suppliers, external consultants, third-party representatives and business partners.

Purpose

The purpose of this policy is to establish the minimum requirements for maintaining clean desks and clear screens and to ensure that, where there is any confidential, restricted or sensitive Information that it is locked away and is out of site or stored on secure cloud storage, as well as to reduce the risks from physical and environmental threats and damage.

It is also to improve the security and confidentiality of information, wherever possible a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. This shall reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended. The purpose of this policy is to set forth the requirements to ensure that all work areas are clear of company information, whether in electronic or paper form.

This policy applies to all permanent, temporary or contracted staff employed by Interr and all who can access information under supervision.

Responsibilities

Information security is everybody's responsibility. Interr Ltd has a responsibility to ensure that the appropriate operational and technical solutions are in place to assist in preventing data breaches from occurring. This policy fulfils a part of that responsibility.

Every person who has access to Interr's data has a personal responsibility to keep the data and information accessed, processed and deleted safe and secure. Should the personal data you access or in your possession be lost, stolen, or compromised it will constitute a breach of the Data Protection Act 2018/GDPR. In the event of a breach, you will have to demonstrate that your actions leading up to the theft, loss or compromise were reasonable.

All breaches will be investigated, reported to the relevant authorities where required and any employee found to have violated this policy may be subjected to disciplinary action in line with Interr's disciplinary procedures.

It is the employee's responsibility to take good care of the computer and any other devices used for work and take all reasonable precautions to ensure that the devices are not damaged, lost or stolen. If the device is stolen, lost or damaged, you must also immediately inform your line manager and HR.

Clear Desk

Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets, or other forms of security furniture when not in use, especially outside working hours. Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office doors must be locked if left unattended. Hard copy documents containing any personal data, or confidential, restricted or sensitive information should only be stored if necessary, for example original legal papers which must be served. Where appropriate, documents should always be scanned to PDF and stored within the dedicated folders on Interr's secure servers/cloud.

Employees are required to ensure that all confidential, restricted, or sensitive information in hardcopy or electronic form is secured at the end of the day and when they are expected to be away from their desk for an extended period. Any confidential, restricted, or sensitive information must be removed from desks and locked in a drawer when a desk is left unoccupied at any time. Confidential, restricted, or sensitive information, when printed, should be cleared from printers immediately. Remove all information from flipcharts and wipe down whiteboards. Confidential waste must not be left on desks, in filing trays or placed in regular waste bins. Any confidential, restricted, or sensitive information received or completed on a paper/printed document, must be scanned into Interr's secure cloud servers and shredded immediately into the designated shredding bags.

Do not write down passwords or other restricted account information on paper or post-it notes and then display them in an accessible location. The company does not permit the use of any removable media, i.e. CDs, DVDs, memory sticks, USB sticks (not limited to) and has implemented locks on the company equipment from them being used.

If you work in a shared office, respect other's privacy and do not invade other's workspace and ensure any confidential easily overheard conversations are not handled in an open room/ shared office but in an area where confidentiality can be followed. Do not peer over other people's shoulders to see what they are working on or intentionally eavesdrop on a short phone call or conversation. You alone are responsible for the data and information you are processing therefore you must ensure that it is safe and secure when you are not at your desk or workstation.

Ensure that if you use a laptop or other portable computer device that it is kept in a secure location at the end of the workday and do not use any personal devices for any company data/use at any time.

The reception area can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times. No personally identifiable information should be kept on desks within reach or sight of visitors and visitors should be accompanied at all times used for access to confidential, restricted or sensitive information must not be left in or on an unattended desk. Keys for desk drawers, cabinets and other secure areas must be stored in the dedicated key safe.

Clear Screen

Computers, laptops, tablets or mobile devices should not be left logged on when unattended and should always be password protected. Computer screens should be facing the wall or angled away from the view of unauthorised persons.

Computer workstations, laptops, tablets or mobile devices must locked at all times when not in use and must be logged off at the end of the working day, to allow security updates to be installed during the evening.

Remain alert of your surroundings and of suspicious behaviours especially when traveling or using all company devices in public. When using the laptop, always keep it with you and in sight, including whilst on break and never leave your device in any public open areas.

Information involved in application services passing over public networks shall be protected from fraudulent activity and modification through the adoption of technical controls e.g. encryption. Using unfamiliar networks are always potentially dangerous and a dynamic risk assessment should be completed before accessing any public network.
You should always try to use your mobile data first as your mobile data is usually encrypted. If you cannot use the mobile phone data, you should only use your only trusted networks, but if you need to use a public network, use a one-time password and then change it as soon as you can, once you're out of the public eye. You should never access any sensitive data when on a public network and log in and/or send information only to website that are fully encrypted (starting with https) from the time you login to the time you log out but do not send files across any public networks. Any files you need to send should be send only when you have a safe network to connect to. Do not use permanently signed in your accounts and sign out as soon as you've finished your work and check forget network after using public network.

Physical and environmental threats

The reliable functioning of electronic equipment and company assets are critical for the success of the company and to ensure the longevity and performance of electronic systems.

The company will complete regular maintenance on the company assets (including PAT testing and PEN and vulnerability testing) to ensure the equipment is safe for use. The data on the electronic equipment is regularly backed up to our cloud services and our systems are monitored.

Our staff and anyone who has access to any company assets/electronic equipment and is required to minimise the risk associated with water damage or flooding by having the equipment strategically elevated above floor level. Proper cable management and visual checks should be completed regularly, including power sockets and/or any extension cables. All cables should be organised and secure to prevent tripping hazards and accident disconnections, help with airflow, and reduce the risks of overheating. Regular temperature regulations to ensure suitable temperature, air conditioning, or heating should be used from extreme heat or cold.

The company also advises all staff not to consume any liquids or food whilst in the vicinity of the company equipment. Smoking and vaping/use of e-cigarettes is strictly prohibited on company or client property.

Paper documentation and transfer of data

All Interr employees always consider whether it is necessary to take any paper records or data containing personal data or other confidential information off site/ away from a protected working environment. Taking paper records off site should only happen when it is absolutely essential to do so and there is no alternative method for accessing or recording the information required. Prior authorisation should be obtained prior from a member of the senior management team.

Where paper records have to be taken off site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed. Where possible, data should be anonymised.

Whilst off site, paper records that are not being actively worked upon must be kept secure and stored separately from encrypted portable laptops which, given their obvious value, are more likely to be of interest to thieves. This applies to paper records temporarily in the employee's home as well as when the employee is on the move.

Where paper records are in transit from one location to another, they should be transported in a way that mitigates the risk of theft or loss and stored in a separate folder away from other valuables, including portable equipment and other electronic devices.

All employees and others covered by the policy are individually responsible for ensuring the adequate protection of all information in their possession and ensuring its safe return.

Statement Review and Assessment

This statement may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024