value one

Developing spaces, delivering smiles.

IT Policy of Value One

Our employees work with a wide range of data every day, from customer details to confidential company information. Our priority is to protect this data as best we can to prevent data espionage and loss.

1. Clean Desk and passwords

At our headquarter, we live a "Clean Desk" policy. This means that we encourage all employees to keep their desks clean and to store sensitive documents securely when they leave their desks. This not only allows for flexible working, but also protects sensitive information from unauthorised access. Computers must always be locked when leaving the workspace.

For us, passwords are an important safeguard against unauthorised access. We ask employees to use unique passwords for different accounts and to change them regularly. Passwords should contain a combination of characters and should never be shared with others. If there is any suspicion that a password has been compromised, it should be changed immediately.

2. Data Storage and disposal

We are committed to secure data storage and disposal. All data must be stored in designated areas, such as network drives or dedicated document management systems. The use of local storage devices such as hard drives or USB sticks is not permitted.

Great care must be taken when disposing of data media. Storage media such as USB sticks, hard drives, SD cards and CDs/DVDs should not be thrown away and must be disposed of safely.

Care must also be taken when disposing of documents. Documents containing sensitive data should not be thrown away, but should be disposed of securely (e.g. shredded). Sensitive data includes all personal data and information whose disclosure or publication could harm the company.

3. Use of internet and emails

The Value One Group places great importance on the safe and responsible use of the internet and email. We urge all employees to exercise caution when surfing the Internet and to limit the sharing of personal information to secure connections.

Email is often a gateway for malware. Employees should not open attachments from unknown or suspicious senders or click on links in emails from untrusted sources. Phishing emails that ask for personal information should be deleted immediately.

If in doubt, our IT department is available to provide support. Employees should also activate the out of office assistant before going away to inform senders of their unavailability.

4. Social Hacking

The Value One Group is aware of the threat of social hacking. This phenomenon refers to the attempt to gain unauthorised access to confidential information or IT systems through the manipulation of individuals. Attackers often pose as employees or representatives of trusted organisations.

Social hacking is often more successful than traditional hacking methods. Therefore, we ask our employees to be extremely cautious about unusual requests over the phone or by email. Confidential information should never be shared without prior verification. The dual control principle must always be applied to financial transactions. Any suspicious activity, warning or error message must be reported immediately to IT.