Blumatix Intelligence GmbH | Schwarzstrasse 48 | 5020 Salzburg
+43 662 243410 | www.blumatix.com | office@blumatix.com

Policy for Home Workplaces

The aim of the directive is to counter potential security risks in the field of information security within our company through standardized regulations and to familiarize all suppliers with IT security-related issues in the home office. This includes in particular:

- The PC/notebook used for data processing must be placed in a separate home office room that is clearly separated from other living areas.

- The home office room must be lockable.

- The screen must be positioned in a way that prevents unauthorized access (both when entering the home office room and through observation from any windows).

- Data on privacy-sensitive storage media must be stored in encrypted form.

- Paper documents must be destroyed when the purpose for their retention no longer exists. Destruction must be carried out in a manner that ensures that relevant data cannot be read by unauthorized persons, for example, using a shredder.

- If documents containing data subject to data secrecy are processed at the home office, they may only be stored in lockable containers outside of telecommuting. This also applies to the transportation of documents between the workplace and the home office.

- Suppliers assigned with telecommuting activities are only allowed to use web browsers for their business activities in the home office and are not permitted to locally store PDF data, images, or screenshots of documents.

- An up-to-date antivirus software must be installed on the PC/notebook.

- Access and login passwords must be changed in accordance with complexity requirements every 90 days.

- The screen lock will be automatically activated after 5 minutes of inactivity and can only be deactivated with appropriate authentication (password entry).

- For further information, please refer to our general IT security directive.