

5 recommendations for SMEs for remote office working

Remote office working means leaving the secure, organised and controlled environment of company premises behind. This situation requires specific technical, organisational and personal measures to ensure business data are kept safe.

Working from home, it is not possible to ensure the same safe and secure infrastructure offered by company premises. Such workplaces at home might just be accessible for family members or visitors. Maybe family members work on the same machine also designed for employees' own work, and with BYOD (bring your own device) strategies, business data can also end up on employees' private devices.

What precautions do I now have to take for my business to handle such particular situations and ensure security? The following five recommendations are meant for businesses with employees working in remote office settings.

Recommendation for employees themselves can be found in our article [“5 recommendations for employees working remotely”](https://www.ebas.ch/en/5-recommendations-for-employees-working-remotely/) (<https://www.ebas.ch/en/5-recommendations-for-employees-working-remotely/>).

1. Remote working policy

Provisions stating how employees must handle confidentiality, integrity and availability of business data are the basis of such a policy and are absolutely vital. It is recommended to record this in a remote working policy which should be communicated to all employees. Such a policy should regulate the following issues:

- General topics such as working hours, response times, work equipment, security measures, back-ups, data protection, data communication, reporting channels, access right to the remote workspace, transfer of information and devices or authorisations.
- Conduct and approach in case of crises: If there are many employees who work remotely and the usual communication channels fail or are impaired, this could result in massive loss of working hours and hence to a very limited resolution of any crisis.

To successfully implement such a policy, it is vital to undertake suitable awareness programs, training and controls.

2. Handling the remote office infrastructure and connections to the company network

Adequate security measures must be prescribed for the remote office infrastructure. Amongst others, this will include handling updates, virus protection, firewall, operating system with user separation, encryption etc. The company should support and advise all remote office employees with regard to securing such devices via their IT support department and security officer. In this respect, connections between remote office devices and the company network must be particularly protected, e. g. using a VPN with 2-factor authentication or an encrypted remote desktop connection.

3. File and data carrier transport

It is inevitable that documents, data carriers and IT devices are moved between company premises and remote office. This means there is a chance of data and devices getting lost, being stolen, read and/or manipulated by unauthorised third parties, leading to a possible loss of confidentiality, integrity and availability. Below some points to be particularly aware of in this regard:

- If at all possible, company devices, data carriers and documents should be moved from the company premises to the remote office directly.
- In case very sensitive (e. g. confidential or potentially even strictly confidential documents, data carriers or company devices) are moved to a remote office, supervisors must be advised of this, the employee moving such items must obtain their authorisation and any such processes must be recorded. Ideally, such sensitive documents should be moved and kept inside a lockable container (e. g. briefcase).

4. Third party access to company data

In case any data worth protecting are processed or stored at a remote office, these must even be protected properly inside any private rooms, too. In case third parties enter such rooms unsupervised, this can compromise the safety of such data. Below some minimum points to be aware of in this regard:

- A remote workplace should be situated inside a specific room exclusively dedicated to professional activities, and in particular must be lockable.
- Confidential documents, data carriers and company devices must be stored inside a remote office inside a lockable area (e. g. cupboard, desk) as soon as they are no longer used for work.

5. Disposal of data carriers and documents

In case there is no suitable disposal option for documents and data carriers available at the remote office, company data could quickly end up in the wrong hands if disposed of inside domestic rubbish or via waste paper collections. Below some points to be particularly aware of in this regard:

- To ensure they are safely erased and can no longer be restored, data carriers and company devices are disposed of exclusively by the company IT department as a matter of course.
- Paper documents must be disposed of correctly in accordance with their level of confidentiality at a remote office, too. Depending on the area of responsibility and requirements, it makes sense to provide any employees involved with a shredder.

Working from home (also called remote working) means more flexible working conditions in terms of space and generally also time. Any work is usually undertaken in a private setting (at home). Such “remote working” is undertaken without a fixed workplace. This article will refer to both these expressions as “remote office” working here.