Work-From-Anywhere cybersecurity checklist

Working remotely poses new challenges for IT and data security. Challenges arise from a general concern for security as well as regulatory compliance. In order to stay safe in any work environment there are certain precautions a company should take. In this paper we collected some of them to help you keep your and your client's data safe.

Checklist data security in remote work

Authentication
Secure authentication to log onto devices and systems must be a priority. This includes secure passwords as well as advanced authentication methods. Multi factor authentication should be the standard, while continuous or dynamic authentication methods are more secure.

Restricted access policies
Employees should have access to all systems and all the data they need to perform their tasks but not more. There should not be one access for all of your applications and databases.

Secure Wifi
In home office environments it is common to use your private wifi. That wifi connection might not have the security standards that are necessary for a business use case, starting with insecure passwords.

Secure VPN
The connection from home offices to the internal company systems should be routed through a secure Virtual Private Network connection. This allows an encrypted and more secure communication between the internal systems and your employees.

Support
In remote work there is much more pressure on each employee to keep data security in mind. Make sure to educate your employees and that you have a permanent contact person in your organization dedicated to cybersecurity questions.

BYOD
Bring your own device (BYOD) is a practice where remote employees use their private devices for work. This should not be a common practice. With private devices there is limited control over necessary security updates and the storage of sensitive data on these devices. When company devices are issued it must be clear what they can be used for privately and what is strictly prohibited e.g. downloading private software not approved by the IT department

Physical access
Remote offices simply don't have the same basic security as offices do. For example in home offices family members often have access to the work desk. Their access to devices must be prohibited and no sensitive data in paper or digital formats should be accessible.

Data storage
Data should be uploaded regularly to a secure company server. No data should be stored internally on private devices or private cloud accounts.

These steps build a necessary basis for secure remote work with sensitive data. Failing to keep your data safe can lead to a data breach which are very costly and can lead to multiple problems in your operations and on the compliance side. In order to stay on top of all things remote work security make sure to follow our blog on Homebase-solutions.com.

Feel free to reach out to us to learn how our solutions can help you achieve data security wherever your employees work from.